

#3

Attorney Docket No. 1341.1102CIP

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Masashi MITOMO, et al.

Application No.:

Group Art Unit:

Filed: February 28, 2002

Examiner:

For: FILTERING APPARATUS, FILTERING METHOD AND COMPUTER PRODUCT

1017 U.S. PTO
10/087807
03/05/02

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application Nos. 2001-388444 and 2001-071214

Filed: December 20, 2001 and March 13, 2001, respectively.

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: February 28, 2002

By: _____

James D. Halsey, Jr.
Registration No. 22,729

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

日 本 国 特 許 庁
JAPAN PATENT OFFICE

J1017 U.S. PRO
10/087807
03/05/02

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年12月20日

出 願 番 号

Application Number:

特願2001-388444

[ST.10/C]:

[JP2001-388444]

出 願 人

Applicant(s):

富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2002年 1月18日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3117351

【書類名】 特許願

【整理番号】 0152846

【提出日】 平成13年12月20日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00
G06F 13/00

【発明の名称】 フィルタリング装置、フィルタリング方法およびこの方法をコンピュータに実行させるプログラム

【請求項の数】 9

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 三友 仁史

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 鳥居 悟

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 小谷 誠剛

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 滝沢 文恵

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 小野 越夫

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通
株式会社内

【氏名】 小谷野 修

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100089118

【弁理士】

【氏名又は名称】 酒井 宏明

【先の出願に基づく優先権主張】

【出願番号】 特願2001- 71214

【出願日】 平成13年 3月13日

【手数料の表示】

【予納台帳番号】 036711

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9717671

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 フィルタリング装置、フィルタリング方法およびこの方法をコンピュータに実行させるプログラム

【特許請求の範囲】

【請求項 1】 クライアントと該クライアントからのアクセス要求に応じてサービスを提供するサーバとの間に介在し、前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡すフィルタリング装置において、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースと、

前記不正パターンデータベースに格納された不正アクセスのパターンおよび所定の見積ルールに基づいて前記アクセス要求の正当性を見積もる見積手段と、

前記見積手段による見積結果および所定の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する判定手段と、

を備えたことを特徴とするフィルタリング装置。

【請求項 2】 前記見積手段は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記判定手段は、前記見積手段により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記見積手段により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする請求項 1 に記載のフィルタリング装置。

【請求項 3】 前記見積手段は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、前記判定手段は、前記見積手段により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを判定することを特徴とする請求項 1 に記載のフィルタリング装置。

【請求項 4】 前記サーバに対する正当アクセスのパターンを格納した正当

パターンデータベースと、前記見積手段による正当性を見積もりの前に、前記アクセス要求が前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定する事前判定手段と、をさらに備え、前記見積手段は、前記事前判定手段により正当アクセスのパターンに該当しないものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする請求項1、2または3に記載のフィルタリング装置。

【請求項5】 所定の外部送信ルールに基づいて、前記判定手段により前記サーバに受け渡さないものと判定されたアクセス要求を所定の外部装置に送信する外部送信手段をさらに備えたことを特徴とする請求項1～4のいずれか一つに記載のフィルタリング装置。

【請求項6】 所定の格納ルールに基づいて、前記判定手段により前記サーバに受け渡さないものと判定されたアクセス要求を所定の格納媒体に格納する格納手段をさらに備えたことを特徴とする請求項1～5のいずれか一つに記載のフィルタリング装置。

【請求項7】 所定の更新ルールに基づいて、前記不正パターンデータベース、正当パターンデータベース、見積ルール、判定ルール、外部送信ルール、格納ルールまたは更新ルールを更新する更新手段をさらに備えたことを特徴とする請求項1～6のいずれか一つに記載のフィルタリング装置。

【請求項8】 クライアントからのアクセス要求に応じてサービスを提供するサーバに対し、前記クライアントからのアクセス要求のうちの正当なアクセス要求のみを受け渡すフィルタリング方法において、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースを参照し、該参照した不正アクセスのパターンおよび所定の見積ルールに基づいて前記アクセス要求の正当性を見積もる見積工程と、

前記見積工程による見積結果および所定の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する判定工程と、

を含んだことを特徴とするフィルタリング方法。

【請求項9】 クライアントからのアクセス要求に応じてサービスを提供するサーバに対し、前記クライアントからのアクセス要求のうちの正当なアクセス

要求のみを受け渡すフィルタリング方法をコンピュータに実行させるプログラムにおいて、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースを参照し、該参照した不正アクセスのパターンおよび所定の見積ルールに基づいて前記アクセス要求の正当性を見積もる見積工程と、

前記見積工程による見積結果および所定の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する判定工程と、

をコンピュータに実行させるプログラム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

この発明は、クライアントと該クライアントからのアクセス要求に応じてサービスを提供するサーバとの間に介在し、前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡すフィルタリング装置、フィルタリング方法およびこの方法をコンピュータに実行させるプログラムに関する。

【 0 0 0 2 】

近時、ネットワーク技術の進展に伴って、インターネット上の分散システムであるWWW (World Wide Web) の利用が急速に拡大し、クライアントからの各種のリクエスト（アクセス要求）に応じて各種のサービスを提供する各種HTTPサーバも累増してきたが、かかるサーバの累増にともなって、クライアントによるサーバへの不正アクセスも増加しつつある。

【 0 0 0 3 】

すなわち、侵入者（イントルーダ）や攻撃者（アタッカ）が企業、団体、個人などのサーバを無権限で不正に利用したり、運用を妨害したり、破壊（クラック）など、サーバを利用する者がその者に与えられた権限により許された行為以外の行為をネットワークを介して意図的におこなうという不正アクセスが増加している。このため、サーバに対する不正アクセスを拒絶することによりサーバの信頼性を確保する必要性が高まりつつある。

【 0 0 0 4 】

【従来の技術】

従来より、クライアントによる不正アクセスからサーバを守るために、インターネットと企業LAN (Local Area Network) との間にファイアウォール (Fire Wall) を構築することが一般的におこなわれている。

【0005】

このファイアウォールは、インターネットに接続したコンピュータやネットワークへの外部からの侵入を防ぐためのソフトウェアであり、企業LANとインターネットの間に、特定のデータやプロトコルだけを通すように設計されたファイアウォール用のコンピュータを置き、LAN内と外部とのデータ交換はすべてこのマシンを通しておこなうことにより、外部からの侵入を防ぐというものである。

【0006】

また、このファイアウォールに関連して、ネットワークベースあるいはホストベースの不正アクセス検知手法がある。前者のネットワークベースの不正アクセス検知手法は、ネットワークを流れる生のパケットを監視することにより不正アクセスを発見するものであり、後者のホストベースの不正アクセス検知手法は、ホストに蓄えられたログ履歴を監視することにより不正アクセスを発見するものである。

【0007】

そして、このような不正アクセス検知手法により発見された不正アクセスに基づいて不正アクセスの送信元クライアントを突き止め、この不正アクセスをおこなったクライアントのIPアドレスなどの送信元情報をファイアウォール用のコンピュータ内に蓄積することにより、この送信元情報を含んだクライアントからのアクセス要求を不正アクセスとして拒絶することがファイアウォールにおいて一般的におこなわれている。

【0008】

【発明が解決しようとする課題】

しかしながら、上記の従来技術は、過去に不正アクセスをおこなったクライアントを不正クライアントと認定し、この不正クライアントからのアクセス要求を不正アクセスとして拒絶するものであるため、不正クライアントと認定された後

の不正アクセスに対してはサーバを防御することができるが、不正クライアントと認定されていないクライアントからの不正アクセスに対してはサーバを防御することができないという問題点があった。すなわち、不正クライアントと認定される前の初回の不正アクセスに対してはサーバを防御することができない。

【 0 0 0 9 】

このため、不正クライアントと認定されていないクライアントからの不正アクセスに対していかにサーバを防御するかが極めて重要な課題となっており、望ましくは、アクセス要求の送信元情報を考慮することなく、正当なアクセス要求であるか不正なアクセス要求であるか否かを判定する枠組みが必要とされている。

【 0 0 1 0 】

そこで、この発明は、上述した従来技術による問題点を解消するためになされたものであり、不正クライアントと認定されていないクライアントからの不正アクセスに対してもサーバを防御することができるフィルタリング装置、フィルタリング方法およびこの方法をコンピュータに実行させるプログラムを提供することを目的とする。

【 0 0 1 1 】

【課題を解決するための手段】

上述した課題を解決し、目的を達成するため、請求項 1、8 または 9 の発明によれば、図 1 に示す見積部 3 2 は、Web サーバ 4 0 に対する不正アクセスのパターンを格納した不正リクエスト DB（データベース）3 3 を参照し、不正アクセスのパターンおよび所定の見積ルール 3 2 a に基づいてクライアント装置 1 0 からのアクセス要求の正当性を見積もり、判定部 3 4 は、見積部 3 2 による見積結果および所定の判定ルール 3 4 a に基づいてアクセス要求を Web サーバ 4 0 に受け渡すか否かを判定することとしたので、アクセス要求の送信元情報ではなくアクセス要求の具体的な要求内容に基づいて不正アクセスであるか否かを判定することができる。これにより、正当なアクセス要求のみを Web サーバ 4 0 に受け渡すことができ、もって不正クライアントと認定されていないクライアント装置 1 0 からの不正アクセスに対しても Web サーバ 4 0 を防御することができる。

【 0 0 1 2 】

また、請求項 2 の発明によれば、図 1 に示す見積部 3 2 は、クライアント装置 1 0 からのアクセス要求が不正リクエスト DB 3 3 に格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、クライアント装置 1 0 からのアクセス要求が不正リクエスト DB 3 3 に格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、判定部 3 4 は、見積部 3 2 により不正アクセスである旨が見積もられたアクセス要求を Web サーバ 4 0 に受け渡さないものと判定するとともに、見積部 3 2 により正当アクセスである旨が見積もられたアクセス要求を Web サーバ 4 0 に受け渡すものと判定することとしたので、アクセス要求が不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを迅速かつ確実に判定することができ、もって不正クライアントと認定されていないクライアント装置 1 0 からの不正アクセスに対しても迅速かつ確実に Web サーバ 4 0 を防御することができる。

【 0 0 1 3 】

また、請求項 3 の発明によれば、図 1 に示す見積部 3 2 は、クライアント装置 1 0 からのアクセス要求が不正リクエスト DB 3 3 に格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、判定部 3 4 は、見積部 3 2 により算出された見積値と所定の閾値とを比較してアクセス要求を Web サーバ 4 0 に受け渡すか否かを判定することとしたので、見積値および閾値の比較によってある程度の幅を持たせて不正アクセスであるか否かを判定することができ、もって不正クライアントと認定されていないクライアント装置 1 0 からの不正アクセスに対してもある程度の幅を持って Web サーバ 4 0 を防御することができる。

【 0 0 1 4 】

また、請求項 4 の発明によれば、図 5 に示す事前判定部 7 1 は、見積部 3 2 による正当性を見積もりの前に、Web サーバ 4 0 に対する正当アクセスのパターンを格納した正当リクエスト DB 7 2 を参照し、クライアント装置 1 0 からのアクセス要求が正当リクエスト DB 7 2 に格納された正当アクセスのパターンのい

ずれかに該当するか否かを判定し、見積部 3 2 は、事前判定部 7 1 により正当アクセスのパターンに該当しないものと判定されたアクセス要求のみについて正当性を見積もることとしたので、正当アクセスのパターンと一致するアクセス要求については正当性を見積もることなく Web サーバ 4 0 に受け渡す一方、正当アクセスのパターンと一致しないアクセス要求のみについて正当性を見積もることができ、もって不正アクセスであるか否かを全体としてより迅速に判定することができる。

【 0 0 1 5 】

また、請求項 5 の発明によれば、図 1 に示す外部通報部 3 7 は、所定の通報ルール 3 7 a に基づいて、判定部 3 4 により Web サーバ 4 0 に受け渡さないものと判定されたアクセス要求を所定の外部装置 5 0 に送信することとしたので、不正アクセスに関する情報を Web サーバ 4 0 の管理者、リクエストフィルタ 3 0 の管理者、サーバ装置 2 0 全体の管理者、ネットワーク全般を監視する公的な機関の管理者などに迅速に通報することができ、もってかかる管理者に対し Web サーバ 4 0 の保全対策を迅速に促すことができる。

【 0 0 1 6 】

また、請求項 6 の発明によれば、図 1 に示すログ管理部 3 6 は、所定の管理ルール 3 6 a に基づいて、判定部 3 4 により Web サーバ 4 0 に受け渡さないものと判定されたアクセス要求を所定の格納媒体 3 6 b に格納することとしたので、格納媒体 3 6 b に格納された不正アクセスに関する情報を分析することなどができ、もって Web サーバ 4 0 の更なる保全対策を講じることができる。

【 0 0 1 7 】

また、請求項 7 の発明によれば、図 1 に示す更新部 3 9 は、所定の更新ルール 3 9 a に基づいて、不正リクエスト DB 3 3、正当リクエスト DB 7 2（図 5 に示す）、見積ルール 3 2 a、判定ルール 3 4 a、通報ルール 3 7 a、管理ルール 3 6 a または更新ルール 3 9 a を更新することとしたので、新たに発見された不正アクセスのパターンを不正リクエスト DB 3 3 に登録することなどができ、もって日々進化する不正アクセスに対して機動的に対応することができる。

【 0 0 1 8 】

【発明の実施の形態】

以下に添付図面を参照して、この発明に係るフィルタリング装置、フィルタリング方法、およびその方法をコンピュータに実行させるプログラムの好適な実施の形態を詳細に説明する。なお、以下に示す実施の形態 1 ～ 3 では、本発明に係るフィルタリング技術を、クライアント装置からの HTTP (HyperText Transfer protocol) リクエストに応じてサービスを提供するサーバ装置に適用した場合について説明する。

【0019】

(実施の形態 1)

本実施の形態 1 では、クライアント装置からの HTTP リクエストが不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを判定する場合について説明する。

【0020】

(1) システムの全体構成

まず最初に、本実施の形態 1 に係るサーバクライアントシステムの構成について説明する。図 1 は、本実施の形態 1 に係るサーバクライアントシステムの構成を示すブロック図である。同図に示すように、本実施の形態 1 に係るサーバクライアントシステムは、Web ブラウザ 11 をそれぞれ有する複数のクライアント装置 10 と、フィルタリング装置としてのリクエストフィルタ 30 および Web サーバ 40 を有するサーバ装置 20 とを、インターネットなどのネットワーク 1 を介して相互に通信可能に接続して構成される。

【0021】

概略的に、このサーバクライアントシステムにあっては、クライアント装置 10 は、Web ブラウザ 11 によりサーバ装置 20 に対して HTTP リクエストなどの各種の処理要求をおこない、サーバ装置 20 の Web サーバ 40 は、クライアント装置 10 からの HTTP リクエストに応じたサービスをクライアント装置 10 に提供する。そして、サーバ装置 20 のリクエストフィルタ 30 は、クライアント装置 10 と Web サーバ 40 との間に介在し、クライアント装置 10 からの HTTP リクエストのうちの正当なリクエストのみを Web サーバ 40 に受け

渡す。

【 0 0 2 2 】

ここで、本実施の形態 1 に係るサーバクライアントシステムは、サーバ装置 20 のリクエストフィルタ 30 によるフィルタリング処理に特徴があり、具体的には、リクエストフィルタ 30 の見積部 32 は、クライアント装置 10 からの HTTP リクエストが不正リクエスト DB 33 に格納された不正アクセスのパターンのいずれかに該当する場合には不正アクセスである旨を見積もり、判定部 34 は、見積部 32 により不正アクセスである旨が見積もられた HTTP リクエストを Web サーバ 40 に受け渡さないものと判定することにより、HTTP リクエストの送信元情報を問題とすることなく、正当な HTTP リクエストのみを Web サーバ 40 に受け渡すことができるように構成している。

【 0 0 2 3 】

(2) クライアント装置の構成

次に、図 1 に示したクライアント装置 10 の構成について説明する。同図に示すように、クライアント装置 10 は、Web ブラウザ 11 を備え、基本的には、サーバ装置 20 に対して HTTP リクエストなどの処理要求をおこない、サーバ装置 20 の Web サーバ 40 により提供される Web データを解釈して、モニタなどの出力部に表示させる表示制御（ブラウズ処理）をおこなう。

【 0 0 2 4 】

そして、このクライアント装置 10 は、悪意を持った使用方法によってサーバ装置 20 に対して不正アクセスをおこなうことができる装置でもある。すなわち、クライアント装置 10 は、侵入者（イントルダ）や攻撃者（アタッカ）などの悪意を持ったユーザの使用によっては、Web サーバ 40 上のパスワードファイルなどのリモートユーザが見るべきでないファイルを見たり、Web サーバ 40 上に存在しないファイルをリクエストして Web サーバ 40 の機能を停止させたり、コマンド文字列を含んだリクエストにより Web サーバ 40 上で任意のシステムコマンドを実行するなどの不正アクセスをおこない得るものである。このようなクライアント装置 10 による不正アクセスに対して Web サーバ 40 を防御するのがリクエストフィルタ 30 の役割である。

【 0 0 2 5 】

なお、クライアント装置 1 0 は、たとえば、パーソナルコンピュータやワークステーション、家庭用ゲーム機、インターネットTV、PDA(Personal Digital Assistant)、あるいは、携帯電話やPHS(Personal Handy Phone System)の如き移動体通信端末によって実現することができる。また、クライアント装置 1 0 は、モデム、TA、ルータなどの通信装置と電話回線を介して、あるいは、専用線を介して、ネットワーク 1 に接続されており、所定の通信規約（たとえば、TCP/IPインターネットプロトコル）に従ってサーバ装置 2 0 にアクセスすることができる。

【 0 0 2 6 】

(3) サーバ装置におけるWebサーバの構成

次に、図 1 に示したサーバ装置 2 0 におけるWebサーバ 4 0 の構成について説明する。同図に示すように、サーバ装置 2 0 のWebサーバ 4 0 は、リクエストフィルタ 3 0 を介してクライアント装置 1 0 からのHTTPリクエストを受信し、このHTTPリクエストに応じてHTML(HyperText Markup Language)などのマークアップ言語により記述された各種の情報を送信するなどのサービスをクライアント装置 1 0 に提供する。

【 0 0 2 7 】

このWebサーバ 4 0 は、機能概念的には、一般的なWebサーバと同様の動作をおこなうものであるが、ここでのWebサーバ 4 0 は、一般的なWebサーバと異なり、サーバ装置 2 0 においてHTTPリクエストに割り当てられるポート番号 8 0 のTCP(Transmission Control Protocol)ポートを監視することはおこなわない。

【 0 0 2 8 】

すなわち、クライアント装置 1 0 からのHTTPリクエストをWebサーバ 4 0 により直接に受信するのではなく、リクエストフィルタ 3 0 がHTTPリクエストを受信し、プロセス間通信をおこなって正当なHTTPリクエストのみをWebサーバ 4 0 に受け渡すこととしている。

【 0 0 2 9 】

(4) サーバ装置におけるリクエストフィルタの構成

次に、図1に示したサーバ装置20におけるリクエストフィルタ30の構成について説明する。同図に示すように、リクエストフィルタ30は、受信部31と、見積部32と、不正リクエストDB33と、判定部34と、送信部35と、ログ管理部36と、外部通報部37と、外部情報取得部38と、更新部39とを備える。

【0030】

このうち、受信部31は、サーバ装置20におけるポート番号80のTCPポートを監視して、クライアント装置10からのHTTPリクエストをWebサーバ40が受信する前に受信する処理部である。なお、受信部31によりクライアント装置10から受信したHTTPリクエストは、見積部32および送信部35に出力される。

【0031】

見積部32は、不正リクエストDB33に格納された不正アクセスのパターンおよび所定の見積ルール32aに基づいてHTTPリクエストの正当性を見積もり、その見積結果を判定部34に出力する処理部である。

【0032】

ここで、見積部32が見積もりに際して参照する不正リクエストDB33について説明する。図2は、不正リクエストDB33に格納される情報の構成例を示す図である。同図に示すように、不正リクエストDB33は、サーバに対する不正アクセスのパターンを格納したデータベースであり、ネットワーク世界で収集された不正アクセスを図示のような形式言語を用いて記述した複数のパターンを記憶している。

【0033】

例えば、同図に示す「URL=</>」のパターンは、URL (Uniform Resource Locator) の先頭が「/」である不正リクエストを意味し、「CGI==p h f、ARG=<Q n a m e = r o o t % O A」のパターンは、CGI (Common Gateway Interface) 名が「p h f」であり、そのある引数の先頭が「Q n a m e = r o o t % O A」である不正リクエストを意味し、「URL<>」.

¥. . ¥. . ¥. . 」のパターンは、URLに「. . ¥. . ¥. . ¥. . 」が含まれる不正リクエストを意味し、「CGI>=. h t r」のパターンは、CGI名の末尾が「. h t r」である不正リクエストを意味する。

【 0 0 3 4 】

なお、図2には示していないが、不正リクエストDB33には、Webサーバ40上で任意のシステムコマンドを実行するような不正なコマンド文字列も複数記憶されている。このようなコマンド文字列のパターンを記憶することにより、攻撃方法が既知である不正アクセスだけでなく、攻撃方法が未知である不正アクセスに対してもWebサーバ40を防御することができる。

【 0 0 3 5 】

このような不正リクエストDB33を参照することにより、見積部32は、所定の見積ルール32aに基づいてHTTPリクエストの正当性を見積もりをおこなう。具体的には、HTTPリクエストが不正リクエストDB33に格納された不正アクセスのパターンのいずれかに該当する場合には、該HTTPリクエストは不正アクセスである旨を見積もり、一方、HTTPリクエストが不正リクエストDB33に格納された不正アクセスのパターンのいずれにも該当しない場合には、該HTTPリクエストは正当アクセスである旨を見積もる。

【 0 0 3 6 】

図1の説明に戻ると、判定部34は、見積部32から受け取った見積結果および所定の判定ルール34aに基づいてHTTPリクエストをWebサーバ40に受け渡すか否かを判定し、この判定結果を送信部35に出力する処理部である。具体的には、見積部32から不正アクセスである旨の見積結果を受け取った場合には、HTTPリクエストをWebサーバ40に受け渡さないものと判定し（不可判定）、一方、見積部32から正当アクセスである旨の見積結果を受け取った場合には、HTTPリクエストをWebサーバ40に受け渡すものと判定する（可判定）。

【 0 0 3 7 】

送信部35は、判定部34から受け取った判定結果に基づいて、受信部31から受け取ったHTTPリクエストの送信を制御する処理部である。具体的には、

判定部 3 4 から可判定を受け取った場合には、H T T P リクエストをプロセス間通信により W e b サーバ 4 0 に受け渡す。一方、判定部 3 4 から不可判定を受け取った場合には、H T T P リクエストの W e b サーバ 4 0 への受け渡しを拒絶して、この不正リクエストを破棄する。

【 0 0 3 8 】

ログ管理部 3 6 は、所定の管理ルール 3 6 a に基づいて、判定部 3 4 により W e b サーバ 4 0 に受け渡さないものと判定された不正リクエストに係る情報を格納媒体 3 6 b に格納して管理する処理部である。具体的には、管理ルール 3 6 a に基づいて、不正リクエストの内容、送信元情報（I P アドレスやホスト名）、送信時刻、見積部 3 2 による見積結果の根拠、判定部 3 4 による判定結果の根拠などの不正リクエストに係る情報を選択的に編集するとともに、この選択編集された情報を不正リクエストの攻撃性の高低などに応じて選択的に格納媒体 3 6 b に格納する。例えば、攻撃性の高い不正リクエストのみを格納するなどである。

【 0 0 3 9 】

なお、格納媒体 3 6 b に格納された情報は、該格納媒体 3 6 b を取り出すことや通信回線を介することなどによりサーバ装置 2 0 の外部に出力することができ、さらに、格納媒体 3 6 b に格納された情報を分析して不正アクセスの傾向などを解析することにより、W e b サーバ 4 0 の更なる保全のために対策を講じることがもできる。

【 0 0 4 0 】

外部通報部 3 7 は、所定の通報ルール 3 7 a に基づいて、判定部 3 4 により W e b サーバ 4 0 に受け渡さないものと判定された不正リクエストに係る情報を外部装置 5 0 に通報する処理部である。具体的には、ログ管理部 3 6 による処理と同様、通報ルール 3 7 a に基づいて、不正リクエストの内容、送信元情報（I P アドレスやホスト名）、送信時刻、見積部 3 2 による見積結果の根拠、判定部 3 4 による判定結果の根拠などの不正リクエストに係る情報を選択的に編集するとともに、この選択編集された情報を不正リクエストの攻撃性の高低などに応じて選択的に外部装置 5 0 に通報する。

【 0 0 4 1 】

この外部通報部 3 7 から通報を受ける外部装置 5 0 は、W e b サーバ 4 0 の管理者、リクエストフィルタ 3 0 の管理者、サーバ装置 2 0 全体の管理者、ネットワーク全般を監視する公的な機関（管理センタ）の管理者など（以下、これらを総称して「管理者」という。）が操作する通信装置である。そして、外部通報部 3 7 は、例えば、攻撃性の高い不正リクエストについてはリアルタイムで迅速に管理者に通報し、攻撃性の低い不正リクエストについては非リアルタイムで一括して管理者に通報するなどして、かかる通報を受ける管理者に対して W e b サーバ 4 0 の保全対策を迅速に促すことができる。

【 0 0 4 2 】

外部情報取得部 3 8 は、所定の取得ルール 3 8 a に基づいて、更新部 3 9 による更新処理に用いられる情報を、外部装置 5 0 や W e b サーバ 4 0 などのリクエストフィルタ 3 0 の外部から能動的または受動的に取得する処理部である。例えば、管理者が外部装置 5 0 を介して入力した新たな不正リクエストのパターンや、管理者が外部装置 5 0 を介して入力した見積ルール 3 2 a の変更指示情報などを取得するほか、不正リクエストによる被害を受けた W e b サーバ 4 0 から被害の状況や不正アクセスの内容などの情報を取得する。なお、所定の取得ルール 3 8 a は、権限が認証された管理者からの情報のみを取得するなどの規則である。

【 0 0 4 3 】

更新部 3 9 は、所定の更新ルール 3 9 a に基づいて、不正リクエスト D B 3 3 、見積ルール 3 2 a 、判定ルール 3 4 a 、管理ルール 3 6 a 、通報ルール 3 7 a 、取得ルール 3 8 a または更新ルール 3 9 a に格納された情報を更新する処理部である。例えば、外部情報取得部 3 8 から新たな不正リクエストのパターンを受け付けた場合には、この不正リクエストのパターンを不正リクエスト D B 3 3 に格納し、また見積ルール 3 2 a の変更指示情報を受け付けた場合には、この変更指示情報に応じて見積ルール 3 2 a を変更する。このような更新処理をおこなうことにより、日々進化する不正アクセスに対して機動的に対応することができる。

【 0 0 4 4 】

（ 5 ）フィルタリング処理

次に、本実施の形態 1 によるフィルタリングの処理手順について説明する。図 3 は、本実施の形態 1 によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置 2 0 におけるリクエストフィルタ 3 0 の受信部 3 1 は、クライアント装置 1 0 からの HTTP リクエストを Web サーバ 4 0 が受信する前に受信する（ステップ S 3 0 1）。

【 0 0 4 5 】

そして、リクエストフィルタ 3 0 の見積部 3 2 は、不正リクエスト DB 3 3 に格納された不正アクセスのパターンおよび所定の見積ルール 3 2 a に基づいて HTTP リクエストの正当性を見積もる（ステップ S 3 0 2）。具体的には、HTTP リクエストが不正アクセスのパターンのいずれかに該当する場合には、不正リクエストである旨を見積もり、一方、HTTP リクエストが不正アクセスのパターンのいずれにも該当しない場合には、正当リクエストである旨を見積もる。

【 0 0 4 6 】

その後、リクエストフィルタ 3 0 の判定部 3 4 は、見積部 3 2 から受け取った見積結果および所定の判定ルール 3 4 a に基づいて HTTP リクエストを Web サーバ 4 0 に受け渡すか否かを判定する（ステップ S 3 0 3）。具体的には、見積部 3 2 により正当なリクエストである旨が見積もられたか否かを判定する。

【 0 0 4 7 】

この判定により、正当なリクエストである旨が見積もられたものと判定された場合には（ステップ S 3 0 3 肯定）、リクエストフィルタ 3 0 の送信部 3 5 は、HTTP リクエストをプロセス間通信により Web サーバ 4 0 に受け渡し（ステップ S 3 0 4）、Web サーバ 4 0 は、HTTP リクエストに応じた情報をクライアント装置 1 0 に送信するなどの正当判定時の処理をおこなう（ステップ S 3 0 5）。

【 0 0 4 8 】

これとは反対に、不正なリクエストである旨が見積もられたものと判定された場合には（ステップ S 3 0 3 否定）、リクエストフィルタ 3 0 の送信部 3 5 は、HTTP リクエストの Web サーバ 4 0 への受け渡しを拒絶し（ステップ S 3 0 6）、リクエストフィルタ 3 0 の各部は、不正リクエストの破棄、格納媒体 3 6

b への格納、外部装置 5 0 への通報などの不正判定時の処理をおこなう（ステップ S 3 0 7）。

【 0 0 4 9 】

上述してきたように、本実施の形態 1 によれば、アクセス要求の送信元情報ではなく、アクセス要求の具体的な要求内容が不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを迅速かつ確実に判定することができる。これにより、不正クライアントと認定されていないクライアント装置 1 0 からの不正アクセスに対しても迅速かつ確実に W e b サーバ 4 0 を防御することができる。

【 0 0 5 0 】

（実施の形態 2）

ところで、上記実施の形態 1 では、クライアント装置からの H T T P リクエストが不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを判定する場合について説明したが、本発明はこれに限定されるものではなく、H T T P リクエストが不正アクセスのパターンに該当する度合に応じて不正アクセスであるか否かを判定する場合についても同様に適用することができる。

【 0 0 5 1 】

そこで、本実施の形態 2 では、H T T P リクエストが不正アクセスのパターンに該当する度合に応じて不正アクセスであるか否かを判定する場合について説明する。なお、本実施の形態 2 においては、サーバクライアントシステムのシステム構成は図 1 に示すものと同様のものとなるので、ここではその詳細な説明を省略する。

【 0 0 5 2 】

まず最初に、本実施の形態 2 の特徴部分である見積部 3 2 および判定部 3 4 について説明する。本実施の形態 2 における見積部 3 2 は、クライアント装置 1 0 からの H T T P リクエストが不正リクエスト D B 3 3 に格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、その見積値を判定部 3 4 に出力する。

【 0 0 5 3 】

具体的には、不正アクセスのパターンから一致するパターンの個数を算出することや、各パターンに危険度を付与して一致するパターンの危険度を算出することなどにより、HTTPリクエストの危険度を示すDI (Danger Index) と呼ばれる見積値を算出する。なお、見積値DIは、例えば1～100の範囲で整数値をとり、危険度が高いHTTPリクエストほど大きな値が算出されるというものである。

【0054】

本実施の形態2における判定部34は、見積部32により算出された見積値DIと所定の閾値とを比較してHTTPリクエストをWebサーバ40に受け渡すか否かを判定し、この判定結果を送信部35に出力する。

【0055】

具体的には、所定の閾値を50と仮定すると、見積部32からDIが50以上である見積値を受け取った場合には、HTTPリクエストをWebサーバ40に受け渡さないものと判定し（不可判定）、一方、見積部32からDIが50未満である見積値を受け取った場合には、HTTPリクエストをWebサーバ40に受け渡すものと判定する（可判定）。

【0056】

次に、本実施の形態2によるフィルタリングの処理手順について説明する。図4は、本実施の形態2によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置20におけるリクエストフィルタ30の受信部31は、クライアント装置10からのHTTPリクエストをWebサーバ40が受信する前に受信する（ステップS401）。

【0057】

そして、リクエストフィルタ30の見積部32は、HTTPリクエストが不正リクエストDB33に格納された不正アクセスのパターンに該当する度合に応じて見積値DIを算出する（ステップS402）。リクエストフィルタ30の判定部34は、見積部32により算出された見積値DIと所定の閾値とを比較してHTTPリクエストをWebサーバ40に受け渡すか否かを判定する（ステップS403）。具体的には、見積値DIが所定の閾値以上であるか否かを判定する。

【 0 0 5 8 】

この判定により、見積値D I が所定の閾値未満であると判定された場合には（ステップS 4 0 3 肯定）、リクエストフィルタ3 0 の送信部3 5 は、H T T P リクエストをプロセス間通信によりW e b サーバ4 0 に受け渡し（ステップS 4 0 4）、W e b サーバ4 0 は、H T T P リクエストに応じた情報をクライアント装置1 0 に送信するなどの正当判定時の処理をおこなう（ステップS 4 0 5）。

【 0 0 5 9 】

これとは反対に、見積値D I が所定の閾値以上であると判定された場合には（ステップS 4 0 3 否定）、リクエストフィルタ3 0 の送信部3 5 は、H T T P リクエストのW e b サーバ4 0 への受け渡しを拒絶し（ステップS 4 0 6）、リクエストフィルタ3 0 の各部は、不正リクエストの破棄、格納媒体3 6 b への格納、外部装置5 0 への通報などの不正判定時の処理をおこなう（ステップS 4 0 7）。

【 0 0 6 0 】

上述してきたように、本実施の形態2 によれば、見積値および閾値の比較によってある程度の幅を持たせて不正アクセスであるか否かを判定することができる。これにより、不正クライアントと認定されていないクライアント装置1 0 からの不正アクセスに対してもある程度の幅を持ってW e b サーバ4 0 を防御することができる。

【 0 0 6 1 】

（実施の形態3）

ところで、上記実施の形態1 および2 では、クライアント装置からの全てのH T T P リクエストについて不正アクセスのパターンに基づく見積もりをおこなう場合について説明したが、本発明にはこれに限定されるものではなく、一部のH T T P リクエストについてのみ見積もりをおこなう場合についても同様に適用することができる。

【 0 0 6 2 】

そこで、本実施の形態3 では、二階層からなるフィルタリング処理をおこない、一部のH T T P リクエストについてのみ不正アクセスのパターンに基づく見積

もりをおこなう場合について説明する。

【 0 0 6 3 】

図 5 は、本実施の形態 3 に係るサーバクライアントシステムの構成を示すブロック図である。なお、図 1 に示した各部と同様の機能を有する部位には同一符号を付すこととしてその詳細な説明を省略し、本実施の形態 3 の特徴部分である事前判定部 7 1 および正当リクエスト DB 7 2 について説明する。

【 0 0 6 4 】

サーバ装置 6 0 におけるリクエストフィルタ 7 0 の事前判定部 7 1 は、見積部 3 2 による正当性を見積もりの前に、正当リクエスト DB 7 2 に格納された正当アクセスのパターンおよび所定の事前判定ルール 7 1 a に基づいて HTTP リクエストの見積もりを省くことができるか否かを判定する処理部である。

【 0 0 6 5 】

ここで、事前判定部 7 1 が判定に際して参照する正当リクエスト DB 7 2 について説明すると、この正当リクエスト DB 7 2 は、Web サーバ 4 0 に対する正当アクセスのパターンを格納したデータベースであり、具体的には、Web サーバ 4 0 上に存在するファイルのうちでリモートユーザに見られても構わないファイルのパスを記憶する。

【 0 0 6 6 】

このリモートユーザに見られても構わないファイルとは、パスワードファイルなどのリモートユーザが見るべきでないファイル以外のファイルであって、例えば、Web サーバ 4 0 に対する HTTP リクエストのリクエスト内容として非常に高い割合を有する画像ファイルなど、不正アクセスの可能性がほとんどないようなファイルが含まれる。

【 0 0 6 7 】

このような正当リクエスト DB 7 2 を参照することにより、事前判定部 7 1 は、所定の事前判定ルール 7 1 a に基づいて HTTP リクエストの見積もりを省くことができるか否かを判定する。具体的には、HTTP リクエストが正当リクエスト DB 7 2 に格納された正当アクセスのパターンのいずれかに該当する場合には、該 HTTP リクエストの見積もりを省くことができるものと判定し、一方、

HTTPリクエストが正当リクエストDB 7 2に格納された正当アクセスのパターンのいずれにも該当しない場合には、該HTTPリクエストの見積もりを省くことができないものと判定する。

【 0 0 6 8 】

そして、事前判定部 7 1 は、見積もりを省くことができないものと判定されたHTTPリクエストのみを見積部 3 2に出力し、見積もりを省くことができるものと判定されたHTTPリクエストについては、見積部 3 2 および判定部 3 4 による処理を省いて、送信部 3 5 を介してWebサーバ 4 0 に受け渡す。

【 0 0 6 9 】

なお、正当リクエストDB 7 2に格納される正当アクセスのパターンは、Webサーバ 4 0 に新たな画像ファイルが追加された場合などに応じて、更新部 3 9 により更新される。

【 0 0 7 0 】

次に、本実施の形態 3 によるフィルタリングの処理手順について説明する。図 6 は、本実施の形態 3 によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置 6 0 におけるリクエストフィルタ 7 0 の受信部 3 1 は、クライアント装置 1 0 からのHTTPリクエストをWebサーバ 4 0 が受信する前に受信する（ステップ S 6 0 1）。

【 0 0 7 1 】

そして、リクエストフィルタ 7 0 の事前判定部 7 1 は、正当リクエストDB 7 2に格納された正当アクセスのパターンおよび所定の事前判定ルール 7 1 a に基づいてHTTPリクエストの見積もりを省くことができるか否かを判定する（ステップ S 6 0 2）。具体的には、HTTPリクエストが正当リクエストDB 7 2に格納された正当アクセスのパターンのいずれかに該当するか否かを判定する。

【 0 0 7 2 】

この判定により、正当アクセスのパターンのいずれかに該当するものと判定された場合には（ステップ S 6 0 2 肯定）、このHTTPリクエストの正当性を見積もりを省き、リクエストフィルタ 7 0 の送信部 3 5 は、HTTPリクエストをプロセス間通信によりWebサーバ 4 0 に受け渡し（ステップ S 6 0 5）、We

bサーバ40は、HTTPリクエストに応じた情報をクライアント装置10に送信するなどの正当判定時の処理をおこなう（ステップS606）。

【0073】

これとは反対に、正当アクセスのパターンのいずれにも該当しないものと判定された場合には（ステップS602否定）、このHTTPリクエストを見積部32に受け渡し、上記実施の形態1または2によるフィルタリング処理と同様の処理をおこなう（ステップS603～608）。

【0074】

すなわち、リクエストフィルタ70の見積部32は、HTTPリクエストの正当性を見積もり（ステップS603）、判定部34は、HTTPリクエストをWebサーバ40に受け渡すか否かを判定する（ステップS604）。

【0075】

この判定により、正当なリクエストである旨が見積もられたものと判定された場合には（ステップS604肯定）、リクエストフィルタ70の送信部35は、HTTPリクエストをプロセス間通信によりWebサーバ40に受け渡し（ステップS605）、Webサーバ40は、HTTPリクエストに応じた情報をクライアント装置10に送信するなどの正当判定時の処理をおこなう（ステップS606）。

【0076】

これとは反対に、不正なリクエストである旨が見積もられたものと判定された場合には（ステップS604否定）、リクエストフィルタ70の送信部35は、HTTPリクエストのWebサーバ40への受け渡しを拒絶し（ステップS607）、リクエストフィルタ70の各部は、不正リクエストの破棄、格納媒体36bへの格納、外部装置50への通報などの不正判定時の処理をおこなう（ステップS608）。

【0077】

上述してきたように、本実施の形態3によれば、画像ファイルを要求するHTTPリクエストのような要求の割合は高いが攻撃性は極めて低いものについては、見積部32および判定部34による処理を省いて迅速な処理をおこなうことが

できるとともに、パスワードファイルやWebサーバ40上に存在しないファイルを要求するHTTPリクエストのような攻撃性が高いものについては、見積部32および判定部34による処理をおこなって、かかる攻撃を有効に防御することができる。

【0078】

なお、本実施の形態1～3では、クライアント装置10からのHTTPリクエストをフィルタリングする場合について説明したが、本発明はこれに限定されるものではなく、FTP (File Transfer Protocol)、telnet、コンソールなど、クライアント装置10からWebサーバ40に入力されるあらゆる情報をフィルタリングする場合に同様に適用することができる。

【0079】

また、本実施の形態1～3では、フィルタリング装置としてのリクエストフィルタ30、70をサーバ装置20、60に設けた場合について説明したが、本発明はこれに限定されるものではなく、例えば、それぞれのクライアント装置側にリクエストフィルタを設けたり、一つのリクエストフィルタにより複数のWebサーバを防御するなど、クライアント装置とWebサーバとの間にリクエストフィルタが介在するあらゆるシステム構成において同様に適用することができる。

【0080】

なお、本実施の形態1～3で説明したフィルタリング方法は、あらかじめ用意されたプログラムをパーソナル・コンピュータやワークステーションなどのコンピュータで実行することによって実現することができる。このプログラムは、インターネットなどのネットワークを介して配布することができる。また、このプログラムは、ハードディスク、フレキシブルディスク(FD)、CD-ROM、MO、DVDなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行することもできる。

【0081】

(実施の形態4)

ところで、上記実施の形態1～3では、サーバに対する不正アクセスのパターンを格納した不正リクエストDB33を参照することによって、アクセス要求の

要求内容から不正アクセスと把握できるアクセス要求を破棄する場合を説明したが、本発明はこれに限定されるものではなく、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求を破棄する場合についても同様に適用することができる。

【0082】

すなわち、サーバに対する不正アクセスとしては、アクセス要求の要求内容から不正アクセスと把握されるアクセス要求の他に、アクセス要求の要求内容からは正当アクセスと把握されるが、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるべきアクセス要求がある。例えば、特定のクライアント装置10からのアクセス要求を集中的に受信している場合や、特定の要求内容からなるアクセス要求を集中的に受信している場合には、個々の要求内容からは正当アクセスと把握されたとしても、アクセス要求の統計からはサーバダウンを狙ったものと考えられるので、不正アクセスとみなされるべきである。

【0083】

そこで、本実施の形態4では、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求に関する情報を格納したデータベースをも参照して正当性を見積もることによって、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求を破棄するフィルタリング処理も実行することができるようにしている。以下、本実施の形態4に係るサーバクライアントシステムにおけるサーバ装置の構成と、本実施の形態4によるフィルタリングの処理手順とを説明する。

【0084】

(1) サーバ装置の構成

まず最初に、本実施の形態4に係るサーバクライアントシステムにおけるサーバ装置の構成を説明する。図7は、本実施の形態4に係るサーバクライアントシステムの構成を示すブロック図である。同図に示すように、本実施の形態4におけるサーバ装置80は、Webサーバ40と、リクエストフィルタ81とを備え、さらに、このリクエストフィルタ81は、受信部31と、第1見積部82と、不正リクエストDB83と、第1判定部84と、第2見積部85と、統計的不正

リクエストDB 8 6と、第2判定部 8 7と、送信部 8 8とを備える。

【0 0 8 5】

このうち、We bサーバ4 0および受信部 3 1は、図1に示した同一符号を付している各部と同様の機能を有する。また、第1見積部 8 2、不正リクエストDB 8 3および第1判定部 8 4は、図1に示した見積部 3 2、不正リクエストDB 3 3および判定部 3 4と同様の機能をそれぞれ有し、上記実施の形態1または2に示したフィルタリング処理と同様の処理、すなわち、HT T Pリクエストの要求内容から不正リクエストと把握できるHT T Pリクエストを破棄するフィルタリング処理（パターンに基づくフィルタリング処理）を実行するものである。

【0 0 8 6】

すなわち、不正リクエストDB 8 3は、サーバに対する不正アクセスのパターンを格納したデータベースである。また、第1見積部 8 2は、不正リクエストDB 8 3に格納された不正アクセスのパターンおよび所定の見積ルール 8 2 aに基づいてHT T Pリクエストの正当性を見積もり、その見積結果（正当リクエスト若しくは不正リクエストである旨の見積結果、または見積値D I）を第1判定部 8 4に出力する。

【0 0 8 7】

さらに、第1判定部 8 4は、第1見積部 8 2から受け取った見積結果および所定の判定ルール 8 4 aに基づいてHT T PリクエストをWe bサーバ4 0に受け渡すか否か（すなわち、正当リクエストである旨が見積もられたか否か、または見積値D Iが所定の閾値以下であるか否か）を判定し、この判定結果を送信部 8 8に出力するか、またはHT T Pリクエストを第2見積部 8 5に出力する。

【0 0 8 8】

これらによって、HT T Pリクエストの要求内容から不正リクエストと把握されたHT T Pリクエスト（すなわち、不正リクエストである旨が見積もられたHT T Pリクエスト、または見積値D Iが所定の閾値以下でなかったHT T Pリクエスト）については、HT T PリクエストをWe bサーバ4 0に受け渡さないものと判定され、不可判定が送信部 8 8に出力されることとなる。

【0 0 8 9】

一方、これらによって、HTTPリクエストの要求内容から不正リクエストと把握されなかったHTTPリクエスト（すなわち、正当リクエストである旨が見積もられたHTTPリクエスト、または見積値DIが所定の閾値以下であったHTTPリクエスト）については、Webサーバ40に対するHTTPリクエストの統計からみて不正リクエストとみなされるHTTPリクエストを破棄するフィルタリング処理（統計に基づくフィルタリング処理）を実行するために、第2見積部85に出力されることとなる。

【0090】

第2見積部85は、統計的不正リクエストDB86に格納された統計的情報および所定の見積ルール85aに基づいてHTTPリクエストの正当性を見積もり、その見積結果を第2判定部87に出力する処理部である。

【0091】

ここで、上記の統計的不正リクエストDB86は、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求に関する情報を格納したデータベースである。具体的には、Webサーバ40に対してHTTPリクエストを送信したクライアント装置10のうち、所定時間内のリクエスト数が所定数を超えたクライアント装置10の送信元情報（IPアドレス）や、Webサーバ40に対して送信されたHTTPリクエストの要求内容のうち、所定時間内のリクエスト数が所定数を超えた要求内容を格納する。

【0092】

このような送信元情報や要求内容を格納することとしたのは、特定のクライアント装置10からのHTTPリクエストを短時間で集中的に受信しているような場合や、特定の要求内容のHTTPリクエストを短時間で集中的に受信しているような場合には、サーバダウンを狙った不正リクエストとみなすことができるからである。

【0093】

そして、第2見積部85は、このような情報を格納した統計的不正リクエストDB86を参照することにより、所定の見積ルール85aに基づいてHTTPリクエストの正当性を見積もりをおこなう。具体的には、HTTPリクエストの送

信元情報が統計的不正リクエストDB 8 6に格納された送信元情報のいずれかに該当する場合、またはHTTPリクエストの要求内容が統計的不正リクエストDB 8 6に格納された要求内容のいずれかに該当する場合には、該HTTPリクエストは不正リクエストである旨を見積もる。

【 0 0 9 4 】

一方、HTTPリクエストの送信元情報が統計的不正リクエストDB 8 6に格納された送信元情報のいずれにも該当しない場合、およびHTTPリクエストの要求内容が統計的不正リクエストDB 8 6に格納された要求内容のいずれかにも該当しない場合には、第2見積部8 5は、該HTTPリクエストは正当リクエストである旨を見積もる。

【 0 0 9 5 】

第2判定部8 7は、第2見積部8 5から受け取った見積結果および所定の判定ルール8 7 aに基づいてHTTPリクエストをWebサーバ4 0に受け渡すか否かを判定し、この判定結果を送信部8 8に出力する処理部である。具体的には、第2見積部8 5から不正リクエストである旨の見積結果を受け取った場合には、HTTPリクエストをWebサーバ4 0に受け渡さないものと判定する（不可判定）。一方、第2見積部8 5から正当リクエストである旨の見積結果を受け取った場合には、HTTPリクエストをWebサーバ4 0に受け渡すものと判定する（可判定）。

【 0 0 9 6 】

送信部8 8は、第1判定部8 4および／または第2判定部8 7から受け取った判定結果に基づいて、受信部3 1から受け取ったHTTPリクエストの送信を制御するアクセス要求受渡手段である。具体的には、第2判定部8 7から可判定を受け取った場合には、HTTPリクエストをプロセス間通信によりWebサーバ4 0に受け渡す。一方、第1判定部8 4または第2判定部8 7から不可判定を受け取った場合には、HTTPリクエストのWebサーバ4 0への受け渡しを拒絶して、この不正リクエストを破棄する。

【 0 0 9 7 】

すなわち、送信部8 8は、第1判定部8 4および第2判定部8 7によりWeb

サーバ 4 0 に受け渡すものと判定された H T T P リクエスト（すなわち、H T T P リクエストの要求内容から不正リクエストと把握されず、かつ、W e b サーバ 4 0 に対する H T T P リクエストの統計からみて不正リクエストとみなされなかった H T T P リクエスト）のみを、正当な H T T P リクエストとして W e b サーバ 4 0 に受け渡す。

【 0 0 9 8 】

なお、図 7 には図示していないが、本実施の形態 4 のリクエストフィルタ 8 1 は、図 1 に示した実施の形態 1 のリクエストフィルタ 3 0 と同様、ログ管理部、外部通信部、外部情報取得部および更新部を備えるものである。すなわち、本実施の形態 4 のリクエストフィルタ 8 1 においては、実施の形態 1 のリクエストフィルタ 3 0 と同様、ログ管理部は、所定の格納ルールに基づいて、送信部 8 8 により W e b サーバ 4 0 に受け渡されなかった H T T P リクエストに係る情報を所定の格納媒体に格納して管理する。

【 0 0 9 9 】

また、外部通信部は、所定の通報ルールに基づいて、送信部 8 8 により W e b サーバ 4 0 に受け渡されなかった H T T P リクエストに係る情報を外部装置に通報する。さらに、外部情報取得部は、所定の取得ルールに基づいて、更新部による更新処理に用いられる情報を、外部装置や W e b サーバ 4 0 などのリクエストフィルタ 8 1 の外部から能動的または受動的に取得する。

【 0 1 0 0 】

そして、更新部は、所定の更新ルールに基づいて、不正リクエスト D B 3 3、見積ルール 3 2 a、判定ルール 3 4 a、見積ルール 8 5 a、判定ルール 8 7 a、管理ルール、通報ルール、取得ルールまたは更新ルールに格納された情報を更新するとともに、所定の更新ルールおよび W e b サーバ 4 0 に対するアクセス要求の統計に基づいて、統計的不正リクエスト D B 8 6 に格納された情報も更新する。

【 0 1 0 1 】

(2) フィルタリング処理

次に、本実施の形態 4 によるフィルタリングの処理手順について説明する。図

8は、本実施の形態4によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置80におけるリクエストフィルタ81の受信部31は、クライアント装置10からのHTTPリクエストをWebサーバ40が受信する前に受信する（ステップS801）。

【0102】

続いて、リクエストフィルタ81は、このHTTPリクエストを第1見積部82に受け渡し、上記実施の形態1または2によるフィルタリング処理と同様の処理、すなわち、パターンに基づくフィルタリング処理を実行する（ステップS802、S803、S808およびS809）。

【0103】

すなわち、第1見積部82は、不正リクエストDB83に格納されたサーバに対する不正アクセスのパターンに基づいて、HTTPリクエストの正当性を見積もり（ステップS802）、第1判定部84は、HTTPリクエストをWebサーバ40に受け渡すか否か（すなわち、正当リクエストである旨が見積もられたか否か、または見積値DIが所定の閾値以下であるか否か）を判定する（ステップS803）。

【0104】

この判定により、HTTPリクエストをWebサーバ40に受け渡さないものと判定された場合（すなわち、不正リクエストである旨が見積もられた場合、または見積値DIが所定の閾値以上である場合）には（ステップS803否定）、送信部88は、HTTPリクエストのWebサーバ40への受け渡しを拒絶する（ステップS808）。さらに、リクエストフィルタ81の各部は、不正リクエストの破棄、格納媒体への格納、外部装置への通報などの不正判定時の処理をおこなう（ステップS809）。

【0105】

これとは反対に、HTTPリクエストをWebサーバ40に受け渡すものと判定された場合（すなわち、正当リクエストである旨が見積もられた場合、または見積値DIが所定の閾値以下である場合）には（ステップS803肯定）、HTTPリクエストは、統計に基づくフィルタリング処理を実行するために、第2見

積部 8 5 に出力される。そして、第 2 見積部 8 5 は、統計的不正リクエスト DB 8 6 に格納された統計的情報および所定の見積ルール 8 5 a に基づいて HTTP リクエストの正当性を見積もる（ステップ S 8 0 4）。

【 0 1 0 6 】

具体的には、第 2 見積部 8 5 は、HTTP リクエストの送信元情報が統計的不正リクエスト DB 8 6 に格納された送信元情報のいずれかに該当する場合、または HTTP リクエストの要求内容が統計的不正リクエスト DB 8 6 に格納された要求内容のいずれかに該当する場合には、該 HTTP リクエストは不正リクエストである旨を見積もる。一方、HTTP リクエストの送信元情報が統計的不正リクエスト DB 8 6 に格納された送信元情報のいずれにも該当しない場合、および HTTP リクエストの要求内容が統計的不正リクエスト DB 8 6 に格納された要求内容のいずれかにも該当しない場合には、第 2 見積部 8 5 は、該 HTTP リクエストは正当リクエストである旨を見積もる。

【 0 1 0 7 】

その後、第 2 判定部 8 7 は、第 2 見積部 8 5 から受け取った見積結果および所定の判定ルール 8 7 a に基づいて HTTP リクエストを Web サーバ 4 0 に受け渡すか否か、すなわち正当リクエストである旨が見積もられたか否かを判定する（ステップ S 8 0 5）。

【 0 1 0 8 】

この判定により、正当リクエストである旨が見積もられた場合には（ステップ S 8 0 5 肯定）、送信部 8 8 は、HTTP リクエストをプロセス間通信により Web サーバ 4 0 に受け渡し（ステップ S 8 0 6）、Web サーバ 4 0 は、HTTP リクエストに応じた情報をクライアント装置 1 0 に送信するなどの正当判定時の処理をおこなう（ステップ S 8 0 7）。

【 0 1 0 9 】

これとは反対に、不正リクエストである旨が見積もられた場合には（ステップ S 8 0 5 否定）、送信部 8 8 は、HTTP リクエストの Web サーバ 4 0 への受け渡しを拒絶し（ステップ S 8 0 8）、リクエストフィルタ 8 1 の各部は、不正リクエストの破棄、格納媒体への格納、外部装置への通報などの不正判定時の処

理をおこなう（ステップ S 8 0 9）。

【 0 1 1 0 】

上記した一連の処理によって、H T T P リクエストの要求内容から不正リクエストと把握されず、かつ、W e b サーバ 4 0 に対する H T T P リクエストの統計からみて不正リクエストとみなされなかった H T T P リクエストのみが、正当な H T T P リクエストとして W e b サーバ 4 0 に受け渡されることとなる。

【 0 1 1 1 】

上述してきたように、本実施の形態 4 によれば、サーバに対する不正アクセスのパターンを格納した不正リクエスト D B 8 3 を参照して正当性を見積もるとともに、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求に関する情報を格納した統計的不正リクエスト D B 8 6 をも参照して正当性を見積もることとしたので、アクセス要求の要求内容から不正アクセスと把握されるアクセス要求のみならず、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求をも破棄することができる。これによって、クライアント装置 1 0 による不正アクセスから W e b サーバ 4 0 を一層確実に防御することができる。

【 0 1 1 2 】

（ 3 ） 本実施の形態 4 の変形例

さて、これまで本実施の形態 4 について説明したが、本発明は上述した実施の形態 4 以外にも、上記特許請求の範囲に記載した技術的思想の範囲内において種々の異なる実施の形態にて実施されてもよいものである。

【 0 1 1 3 】

例えば、本実施の形態 4 では、統計的不正リクエスト D B 8 6 が所定の送信元情報および要求内容を格納する場合を説明したが、本発明はこれに限定されるものではなく、統計的不正リクエスト D B 8 6 が所定の送信元情報または要求内容のいずれか一方を格納する場合にも同様に適用することができる。

【 0 1 1 4 】

すなわち、統計的不正リクエスト D B 8 6 が所定の送信元情報のみを記憶する場合には、第 2 見積部 8 5 は、H T T P リクエストの送信元情報が統計的不正リ

クエストDB86に格納された送信元情報のいずれかに該当することを条件に該アクセス要求は不正アクセスである旨を見積もるとともに、いずれにも該当しないことを条件に該アクセス要求は正当アクセスである旨を見積もることとなる。

【0115】

一方、統計的不正リクエストDB86が所定の要求内容のみを記憶する場合には、第2見積部85は、HTTPリクエストの要求内容が統計的不正リクエストDB86に格納された要求内容のいずれかに該当することを条件に該アクセス要求は不正アクセスである旨を見積もるとともに、いずれにも該当しないことを条件に該アクセス要求は正当アクセスである旨を見積もることとなる。

【0116】

また、本実施の形態4では、HTTPリクエストの送信元情報や要求内容が、統計的不正リクエストDB86に格納された所定の送信元情報や要求内容に該当するか否かによって不正アクセスであるか否かを判定する場合について説明したが、本発明はこれに限定されるものではなく、統計的不正リクエストDB86に格納された所定の送信元情報や要求内容に該当する度合に応じて不正アクセスであるか否かを判定する場合にも同様に適用することができる。

【0117】

すなわち、この場合には、上記実施の形態2と同様、統計的不正リクエストDB86に格納された所定の送信元情報や要求内容にそれぞれ危険度を付与しておき、第2見積部85は、HTTPリクエストの送信元情報や要求内容に対応する危険度を用いて、HTTPリクエストの危険度を示すDI (Danger Index) と呼ばれる見積値を算出し、第2判定部87は、この算出された見積値DIと所定の閾値とを比較して不正アクセスであるか否かを判定することとなる。

【0118】

また、本実施の形態4では、第2見積部85が、第1判定部84によりWebサーバ40に受け渡すものと判定されたHTTPリクエストのみについて正当性を見積もる場合、すなわち、パターンに基づくフィルタリング処理を実行した後に、統計に基づくフィルタリング処理を実行する場合を説明したが、本発明はこれに限定されるものではない。

【 0 1 1 9 】

例えば、第 1 見積部 8 2 が、第 2 判定部 8 7 により W e b サーバ 4 0 に受け渡すものと判定された H T T P リクエストのみについて正当性を見積もる場合にも同様に適用することができる。この場合には、統計に基づくフィルタリング処理を実行した後に、パターンに基づくフィルタリング処理を実行することとなる。

【 0 1 2 0 】

また、例えば、上記実施の形態 3 で説明した事前判定処理を追加し、事前判定部が、第 2 判定部 8 7 により W e b サーバ 4 0 に受け渡すものと判定されたアクセス要求のみについて事前判定処理をおこなう場合にも同様に適用することができる。この場合には、統計に基づくフィルタリング処理を実行した後に、事前判定処理がおこなわれ、この事前判定処理に続いて、パターンに基づくフィルタリング処理を実行することとなる。

【 0 1 2 1 】

なお、事前判定処理を追加する場合には、統計に基づくフィルタリング処理よりも後に事前判定処理をおこなう必要がある。この統計に基づくフィルタリング処理よりも前に事前判定処理をおこなうと、上記のような H T T P リクエストが正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するものと判定されてしまい、統計に基づくフィルタリング処理によって破棄されることなく、W e b サーバ 4 0 に受け渡されるおそれが生じるからである。

【 0 1 2 2 】

さらに、本発明は、パターンに基づくフィルタリング処理や統計に基づくフィルタリング処理を階層的に実行する場合に限定されず、これらの各処理を並列的に実行する場合にも同様に適用することができる。すなわち、この場合には、図 9 に示すように、サーバ装置 9 0 のリクエストフィルタ 9 1 は、受信部 3 1 と送信部 8 8 との間に、パターンに基づくフィルタリング処理を実行する第 1 見積部 8 2 および第 1 判定部 8 4 と、統計に基づくフィルタリング処理を実行する第 2 見積部 8 5 および第 2 判定部 8 7 とを、並列的に備えることとなる。このようなリクエストフィルタ 9 1 を構成することにより、不正アクセスであるか否かを一層迅速に判定することが可能になる。

【 0 1 2 3 】

(実施の形態 5)

ところで、上記実施の形態 4 では、統計的不正リクエスト DB 8 6 を参照して統計に基づくフィルタリング処理を実行する場合を説明したが、本発明は、この統計的不正リクエスト DB 8 6 に格納された情報を動的に更新しながら、フィルタリング処理を実行することもできる。

【 0 1 2 4 】

すなわち、実施の形態 4 では、第 2 見積部 8 5 は、HTTP リクエストの送信元情報が統計的不正リクエスト DB 8 6 に格納された送信元情報のいずれかに該当する場合、または HTTP リクエストの要求内容が統計的不正リクエスト DB 8 6 に格納された要求内容のいずれかに該当する場合には、該 HTTP リクエストは不正リクエストである旨を見積もることとしている。

【 0 1 2 5 】

しかしながら、特定のクライアント装置 1 0 (送信元情報)からの HTTP リクエストや特定の要求内容の HTTP リクエストの受信が急激に増加しているような状況において、この特定の送信元情報や要求内容が統計的不正リクエスト DB 8 6 にリアルタイムで追加されなかったのでは、サーバに対する HTTP リクエストの統計からみて不正リクエストとみなされる HTTP リクエストが Web サーバ 4 0 に送信されてしまう。

【 0 1 2 6 】

その一方で、統計的不正リクエスト DB 8 6 に格納された特定の送信元情報や要求内容の HTTP リクエストの受信が減少しているような状況において、この特定の送信元情報や要求内容が統計的不正リクエスト DB 8 6 からリアルタイムで削除されなかったのでは、サーバに対する HTTP リクエストの統計からみて不正リクエストとはみなされない HTTP リクエストまでが破棄されてしまう。

【 0 1 2 7 】

そこで、本実施の形態 5 では、統計的不正リクエスト DB 8 6 に格納された情報を動的に更新することによって、サーバに対する HTTP リクエストの統計からみて不正リクエストとみなされる HTTP リクエストを精度良く確実に破棄す

ることができるようにしている。以下、本実施の形態 5 に係るサーバクライアントシステムにおけるサーバ装置の構成を説明する。

【0128】

図 10 は、本実施の形態 5 に係るサーバクライアントシステムの構成を示すブロック図である。なお、図 1 または図 7 に示した各部と同様の機能を有する部位には同一符号を付すこととしてその詳細な説明を省略し、本実施の形態 5 の特徴部分であるアクセス管理部 102 および動的更新部 103 について説明する。

【0129】

サーバ装置 100 におけるリクエストフィルタ 101 のアクセス管理部 102 は、サーバ装置 100 に対して送信された HTTP リクエストの送信元情報、要求内容および送信時刻を履歴として管理するメモリである。

【0130】

そして、動的更新部 103 は、アクセス管理部 102 により管理される情報および所定の更新ルール 103a に基づいて、統計的不正リクエスト DB 86 に格納された情報を動的に更新する処理部である。具体的には、アクセス管理部 102 を参照し、特定のクライアント装置 10 から Web サーバ 40 に対して送信された所定時間内の HTTP リクエスト数が所定の上限数を超えた場合には、この送信元情報を統計的不正リクエスト DB 86 に追加する。

【0131】

その一方で、動的更新部 103 は、統計的不正リクエスト DB 86 に格納された送信元情報のクライアント装置 10 から Web サーバ 40 に対して送信された所定時間内の HTTP リクエスト数が所定の下限数を下回った場合には、この送信元情報を統計的不正リクエスト DB 86 から削除する。

【0132】

さらに、動的更新部 103 は、アクセス管理部 102 を参照し、Web サーバ 40 に対して送信された特定の HTTP リクエストのリクエスト数が所定時間内に所定の上限数を超えた場合には、この HTTP リクエストの要求内容を統計的不正リクエスト DB 86 に追加する一方、統計的不正リクエスト DB 86 に格納された要求内容の HTTP リクエストのリクエスト数が所定時間内に所定の下限

数を下回った場合には、この要求内容を統計的不正リクエストDB 8 6 から削除する。

【0 1 3 3】

なお、上記した「所定の上限数」は、これを超えた場合にはサーバダウンを狙った不正アクセスとみなれるべきという閾値であり、一方、上記した「所定の下限数」は、これを下回った場合にはサーバダウンを狙った不正アクセスとみなれるべきでないという閾値である。そして、これらの上限数および下限数は、Webサーバ4 0 の処理能力などを考慮して設定される。

【0 1 3 4】

上述してきたように、本実施の形態5によれば、所定時間内にWebサーバ4 0 に対してHTTPリクエストを送信した各クライアント装置1 0 ごとのリクエスト数や、所定時間内にWebサーバ4 0 に対して送信されたHTTPリクエストの各要求内容ごとのリクエスト数に応じて、統計的不正リクエストDB 8 6 に格納される送信元情報や要求内容を追加したり削除することとしたので、Webサーバ4 0 に対するHTTPリクエストの統計からみて不正リクエストとみなされるHTTPリクエストを精度良く確実に破棄することができる。

【0 1 3 5】

なお、本実施の形態5では、統計的不正リクエストDB 8 6 に格納される送信元情報および要求内容をともに更新する場合を説明したが、本発明はこれに限定されるものではなく、統計的不正リクエストDB 8 6 に送信元情報または要求内容のいずれか一方を格納する場合には、格納される送信元情報または要求内容のみを追加したり削除するなど、統計的不正リクエストDB 8 6 に格納される情報に応じて更新することができる。

【0 1 3 6】

また、本実施の形態5では、アクセス管理部1 0 2 のみを参照して、統計的不正リクエストDB 8 6 を動的に更新する場合を説明したが、本発明はこれに限定されるものではなく、例えば、ログ管理部3 6 およびアクセス管理部1 0 2 の両者を参照して、統計的不正リクエストDB 8 6 を動的に更新する場合にも同様に適用することができる。

【0137】

すなわち、ログ管理部36に追加された送信元情報を統計的不正リクエストDB86にも追加したり、また、ログ管理部36に格納されている送信元情報については、統計的不正リクエストDB86において高度の危険度を付与したり、さらに、リクエスト数が所定の下限値を下回った場合でも、統計的不正リクエストDB86から削除しないなど、ログ管理部36をも参照して統計的不正リクエストDB86を動的に更新することができる。

【0138】

(実施の形態6)

ところで、上記実施の形態1～5では、クライアント装置10から送信されたHTTPリクエストに対して種々の見積もりをおこなって不正アクセスを破棄する場合を説明したが、本発明はこれに限定されるものではなく、HTTPリクエストに応じてWebサーバ40からクライアント装置10に送信されるレスポンスに対しても、その正当性を見積もって不正なレスポンスを破棄することもできる。

【0139】

すなわち、上記実施の形態1～5では、不正リクエストのパターンを不正リクエストDB33などに格納し、クライアント装置10からのHTTPリクエストが不正リクエストのパターンに一致するか否かなどによって不正アクセスであるか否かを判定したが、不正リクエストのなかには、パターンとして記述し難い不正リクエストもある。例えば、Webサーバ40が所有しないファイルを要求するHTTPリクエストを送信することによって、ディレクトリ情報など、Webサーバ40の外部に漏れてはいけない秘匿情報をレスポンスとして受信しようとする不正アクセスなどである。

【0140】

このような不正アクセスは、Webサーバ40が所有しないファイルを要求するものであるところ、パターンとして記述し難いため、不正リクエストのパターンに一致するか否かなどを見積もるだけでは、これを不正アクセスと判定することができない。一方、このような不正アクセスに応じてWebサーバ40からク

クライアント装置 1 0 に送信されるレスポンスには、ディレクトリ情報など、Webサーバ 4 0 の外部に漏れてはいけない秘匿情報が含まれるので、このような秘匿情報がレスポンスに含まれるか否かを見積もれば、パターンとして記述し難い不正アクセスに対しても対応することができると考えられる。

【0 1 4 1】

そこで、本実施の形態 6 では、クライアント装置 1 0 に対して送信されるべきでない不正レスポンスのパターンを格納したデータベースを参照して、レスポンスの正当性を見積もることによって、パターンとして記述し難い不正アクセスに応じてクライアント装置 1 0 に送信されようとする不正なレスポンスをも破棄することができるようにしている。以下、本実施の形態 6 に係るサーバクライアントシステムにおけるサーバ装置の構成と、本実施の形態 6 によるフィルタリングの処理手順とを説明する。

【0 1 4 2】

(1) サーバ装置の構成

まず最初に、本実施の形態 6 に係るサーバクライアントシステムにおけるサーバ装置の構成を説明する。図 1 1 は、本実施の形態 6 に係るサーバクライアントシステムの構成を示すブロック図である。同図に示すように、本実施の形態 6 におけるサーバ装置 1 1 0 は、Webサーバ 4 0 と、リクエストフィルタ 1 1 1 とを備え、さらに、このリクエストフィルタ 1 1 1 は、受信部 3 1 と、見積部 3 2 と、不正リクエスト DB 3 3 と、判定部 3 4 と、送信部 3 5 と、レスポンス受信部 1 1 2 と、レスポンス見積部 1 1 3 と、不正レスポンス DB 1 1 4 と、レスポンス判定部 1 1 5 と、レスポンス送信部 1 1 6 とを備える。

【0 1 4 3】

このうち、受信部 3 1、見積部 3 2、不正リクエスト DB 3 3、判定部 3 4 および送信部 3 5 は、図 1 に示した同一符号を付している各部と同様の機能を有し、上記実施の形態 1 または 2 に示したフィルタリング処理と同様の処理、すなわち、パターンに基づくフィルタリング処理を実行するものである。

【0 1 4 4】

ところで、Webサーバ 4 0 が所有しないファイルを要求する HTTP リクエ

ストなど、不正アクセスのパターンとして記述することが困難なHTTPリクエストについては、不正リクエストDB33にはパターンとして格納されないもので、不正リクエストとして破棄されることなく、Webサーバ40に送信されることとなる。しかしながら、かかる不正リクエストに応じてWebサーバ40からクライアント装置10に送信されようとするレスポンスは、以下に説明する各部の処理によって、不正なレスポンスとして破棄される。

【0145】

レスポンス受信部112は、Webサーバ40からのレスポンスをクライアント装置10に送信する前に受信する処理部である。なお、レスポンス受信部112によりWebサーバ40から受信したレスポンスは、レスポンス見積部113およびレスポンス送信部116に出力される。

【0146】

レスポンス見積部113は、不正レスポンスDB114に格納された不正レスポンスのパターンおよび所定の見積ルール113aに基づいてレスポンスの正当性を見積もり、その見積結果をレスポンス判定部115に出力する処理部である。

【0147】

ここで、上記の不正レスポンスDB114は、HTTPリクエストに応じてWebサーバ40からクライアント装置10に対してサービスとして送信されるレスポンスのうち、クライアント装置10に対して送信されるべきでない不正レスポンスのパターンを格納したデータベースである。具体的には、ディレクトリ情報など、Webサーバ40の外部に漏れてはいけない秘匿情報をパターンとして記憶する。

【0148】

これらの秘匿情報をパターンとして記憶することとしたのは、Webサーバ40が所有しないファイルを要求するHTTPリクエストに対するレスポンスとして、これらの秘匿情報がクライアント装置10に送信されるおそれがあるからである。

【0149】

そして、レスポンス見積部 1 1 3 は、このような秘匿情報を格納した不正レスポンス DB 1 1 4 を参照することにより、所定の見積ルール 1 1 3 a に基づいてレスポンスの正当性を見積もりをおこなう。具体的には、レスポンスが不正レスポンス DB 1 1 4 に格納された秘匿情報パターンのいずれかに該当する場合には、該レスポンスは不正レスポンスである旨を見積もり、一方、レスポンスが不正レスポンス DB 1 1 4 に格納された秘匿情報パターンのいずれにも該当しない場合には、該レスポンスは正当レスポンスである旨を見積もる。

【 0 1 5 0 】

レスポンス判定部 1 1 5 は、レスポンス見積部 1 1 3 から受け取った見積結果および所定の判定ルール 1 1 5 a に基づいてレスポンスをクライアント装置 1 0 に送信するか否かを判定し、この判定結果をレスポンス送信部 1 1 6 に出力する処理部である。具体的には、レスポンス見積部 1 1 3 から不正レスポンスである旨の見積結果を受け取った場合には、レスポンスをクライアント装置 1 0 に送信しないものと判定し（不可判定）、一方、レスポンス見積部 1 1 3 から正当レスポンスである旨の見積結果を受け取った場合には、レスポンスをクライアント装置 1 0 に送信するものと判定する（可判定）。

【 0 1 5 1 】

レスポンス送信部 1 1 6 は、レスポンス判定部 1 1 5 から受け取った判定結果に基づいて、レスポンス受信部 1 1 2 から受け取ったレスポンスの送信を制御する処理部である。具体的には、レスポンス判定部 1 1 5 から可判定を受け取った場合には、レスポンスをネットワーク 1 を介してクライアント装置 1 0 に送信する。一方、レスポンス判定部 1 1 5 から不可判定を受け取った場合には、レスポンスのクライアント装置 1 0 への送信を拒絶して、このレスポンスを不正レスポンスとして破棄する。

【 0 1 5 2 】

なお、図 7 には図示していないが、本実施の形態 6 のリクエストフィルタ 1 1 1 は、図 1 に示した実施の形態 1 のリクエストフィルタ 3 0 と同様、ログ管理部、外部通信部、外部情報取得部および更新部を備えるものである。すなわち、本実施の形態 6 のリクエストフィルタ 1 1 1 においては、実施の形態 1 のリクエス

トフィルタ 3 0 と同様、ログ管理部は、所定の格納ルールに基づいて、レスポンス送信部 1 1 6 によりクライアント装置 1 0 に送信されなかったレスポンスに係る情報や、このレスポンスの起因となった H T T P リクエストに係る情報を所定の格納媒体に格納して管理する。

【 0 1 5 3 】

また、外部通信部は、所定の通報ルールに基づいて、レスポンス送信部 1 1 6 によりクライアント装置 1 0 に送信されなかったレスポンスに係る情報や、このレスポンスの起因となった H T T P リクエストに係る情報を外部装置に通報する。さらに、外部情報取得部は、所定の取得ルールに基づいて、更新部による更新処理に用いられる情報を、外部装置や W e b サーバ 4 0 などのリクエストフィルタ 1 1 1 の外部から能動的または受動的に取得する。

【 0 1 5 4 】

そして、更新部は、所定の更新ルールに基づいて、不正レスポンス D B 1 1 4 、見積ルール 1 1 3 a 、判定ルール 1 1 5 a 、管理ルール、通報ルール、取得ルールまたは更新ルールに格納された情報を更新する。例えば、外部情報取得部から新たな不正レスポンスのパターンを受け付けた場合には、この不正レスポンスのパターンを不正レスポンス D B 1 1 4 に格納し、また見積ルール 1 1 3 a の変更指示情報を受け付けた場合には、この変更指示情報に応じて見積ルール 1 1 3 a を変更する。

【 0 1 5 5 】

(2) フィルタリング処理

次に、本実施の形態 6 によるフィルタリングの処理手順について説明する。図 1 2 は、本実施の形態 6 によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置 1 1 0 におけるリクエストフィルタ 1 1 1 の受信部 3 1 は、クライアント装置 1 0 からの H T T P リクエストを W e b サーバ 4 0 が受信する前に受信する（ステップ S 1 2 0 1 ）。

【 0 1 5 6 】

続いて、リクエストフィルタ 1 1 1 は、この H T T P リクエストを見積部 3 2 に受け渡し、上記実施の形態 1 または 2 によるフィルタリング処理と同様の処理

、すなわち、パターンに基づくフィルタリング処理を実行する（ステップ S 1 2 0 2 ～ S 1 2 0 5、ステップ S 1 2 1 0 および S 1 2 1 1）。

【 0 1 5 7 】

すなわち、見積部 3 2 は、不正リクエスト DB 3 3 に格納されたサーバに対する不正アクセスのパターンに基づいて、HTTP リクエストの正当性を見積もり（ステップ S 1 2 0 2）、判定部 3 4 は、HTTP リクエストを Web サーバ 4 0 に受け渡すか否か（すなわち、正当リクエストである旨が見積もられたか否か、または見積値 DI が所定の閾値以下であるか否か）を判定する（ステップ S 1 2 0 3）。

【 0 1 5 8 】

この判定により、HTTP リクエストを Web サーバ 4 0 に受け渡さないものと判定された場合（すなわち、不正リクエストである旨が見積もられた場合、または見積値 DI が所定の閾値以上である場合）には（ステップ S 1 2 0 3 否定）、送信部 3 5 は、HTTP リクエストの Web サーバ 4 0 への受け渡しを拒絶する（ステップ S 1 2 1 0）。さらに、リクエストフィルタ 1 1 1 の各部は、不正リクエストの破棄、格納媒体への格納、外部装置への通報などの不正判定時の処理をおこなう（ステップ S 1 2 1 1）。

【 0 1 5 9 】

これとは反対に、正当リクエストである旨が見積もられた場合には（ステップ S 1 2 0 3 肯定）、送信部 3 5 は、HTTP リクエストをプロセス間通信により Web サーバ 4 0 に送信し（ステップ S 1 2 0 4）、Web サーバ 4 0 は、HTTP リクエストに応じたレスポンスを作成するなど、正当判定時の処理をおこなう（ステップ S 1 2 0 5）。

【 0 1 6 0 】

続いて、リクエストフィルタ 1 1 1 のレスポンス受信部 1 1 2 は、Web サーバ 4 0 からレスポンスを受信する（ステップ S 1 2 0 6）。そして、レスポンス見積部 1 1 3 は、不正レスポンス DB 1 1 4 に格納された秘匿情報パターンおよび所定の見積ルール 1 1 3 a に基づいてレスポンスの正当性を見積もる（ステップ S 1 2 0 7）。具体的には、レスポンスが不正レスポンス DB 1 1 4 に格納さ

れた秘匿情報パターンのいずれかに該当する場合には、該レスポンスは不正レスポンスである旨を見積もり、一方、レスポンスが不正レスポンスDB 1 1 4 に格納された秘匿情報パターンのいずれにも該当しない場合には、該レスポンスは正当レスポンスである旨を見積もる。

【0 1 6 1】

その後、レスポンス判定部 1 1 5 は、レスポンス見積部 1 1 3 から受け取った見積結果および所定の判定ルール 1 1 5 a に基づいて、レスポンスをクライアント装置 1 0 に送信するか否かを判定する（ステップ S 1 2 0 8）。具体的には、正当なレスポンスとして見積もられたか否かを判定する。

【0 1 6 2】

この判定により、正当なレスポンスである旨が見積もられたものと判定された場合には（ステップ S 1 2 0 8 肯定）、レスポンス送信部 1 1 6 は、レスポンスをネットワーク 1 を介してクライアント装置 1 0 に送信する（ステップ S 1 2 0 9）。

【0 1 6 3】

これとは反対に、不正なレスポンスである旨が見積もられたものと判定された場合には（ステップ S 1 2 0 8 否定）、レスポンス送信部 1 1 6 は、レスポンスのクライアント装置 1 0 への送信を拒絶し（ステップ S 1 2 1 2）、リクエストフィルタ 1 1 1 の各部は、不正レスポンスの破棄、格納媒体への格納、外部装置への通報など、不正判定時の処理をおこなう（ステップ S 1 2 1 3）。

【0 1 6 4】

上記した一連の処理によって、正当なアクセスに応じた正当なレスポンス、すなわち不正アクセスとして破棄されず、かつ、不正レスポンスとして破棄されなかったレスポンスのみが、クライアント装置 1 0 に送信されることとなる。

【0 1 6 5】

上述してきたように、本実施の形態 6 によれば、クライアント装置 1 0 から送信された HTTP リクエストに対して種々の見積もりをおこなって不正アクセスを破棄するとともに、HTTP リクエストに応じて Web サーバ 4 0 からクライアント装置 1 0 に送信されるレスポンスに対しても、その正当性を見積もって不

正なレスポンスを破棄することとしたので、不正アクセスのパターンとして記述される不正アクセスのみならず、不正アクセスのパターンとして記述し難い不正アクセスに応じた不正なレスポンスをも破棄することができる。これによって、クライアント装置 1 0 による不正アクセスから W e b サーバ 4 0 を一層確実に防御することができる。

【 0 1 6 6 】

(3) 本実施の形態 6 の変形例

さて、これまで本実施の形態 6 について説明したが、本発明は上述した実施の形態 6 以外にも、上記特許請求の範囲に記載した技術的思想の範囲内において種々の異なる実施の形態にて実施されてもよいものである。

【 0 1 6 7 】

例えば、本実施の形態 6 では、W e b サーバ 4 0 からのレスポンスが不正レスポンス D B 1 1 4 に格納された不正レスポンスのパターンに該当するか否かによって不正レスポンスであるか否かを判定する場合について説明したが、本発明はこれに限定されるものではなく、不正レスポンス D B 1 1 4 に格納された不正レスポンスのパターンに該当する度合に応じて不正レスポンスであるか否かを判定する場合にも同様に適用することができる。

【 0 1 6 8 】

すなわち、この場合には、上記実施の形態 2 と同様、レスポンス見積部 1 1 3 は、不正レスポンス D B 1 1 4 に格納された不正レスポンスのパターンから一致するパターンの個数を算出することや、各パターンに危険度を付与して一致するパターンの危険度を算出することなどにより、レスポンスの危険度を示す D I (Danger Index) と呼ばれる見積値を算出し、レスポンス判定部 1 1 5 は、この算出された見積値と所定の閾値とを比較してレスポンスをクライアント装置 1 0 に送信するか否かを判定することとなる。

【 0 1 6 9 】

また、本実施の形態 6 では、クライアント装置 1 0 から送信された H T T P リクエストに対しては、パターンに基づくフィルタリング処理を実行する場合を説明したが、本発明はこれに限定されるものではなく、上記実施の形態 3 で説明し

た事前判定処理や、上記実施の形態 4 で説明した統計に基づくフィルタリング処理をともに実行する場合にも同様に適用することができる。

【 0 1 7 0 】

(実施の形態 7)

ところで、上記実施の形態 1 ～ 6 では、暗号処理されていない H T T P リクエストや暗号処理されていないレスポンスに対してフィルタリング処理を実行する場合を説明したが、本発明はこれに限定されるものではなく、暗号処理がなされた H T T P リクエストや暗号処理がなされたレスポンスに対してフィルタリング処理を実行する場合にも同様に適用することができる。

【 0 1 7 1 】

すなわち、上記実施の形態 1 ～ 6 では、W e b サーバ 4 0 が、クライアント装置 1 0 から暗号処理されていない H T T P リクエストを受信するとともに、暗号処理されていないレスポンスをクライアント装置 1 0 に送信することを前提にしている。しかしながら、W e b サーバ 4 0 によっては、提供するサービスの秘匿性などを確保するために、クライアント装置 1 0 から暗号処理がなされた H T T P リクエストを受信するとともに、暗号処理がなされたレスポンスをクライアント装置 1 0 に送信するようにしたものもある。

【 0 1 7 2 】

このような W e b サーバ 4 0 に対して、上記実施の形態 1 ～ 6 で説明したフィルタリング処理を単純に適用したのでは、暗号化がなされた不正アクセスや暗号化がなされた不正レスポンスを破棄することはできない。このため、不正アクセスから W e b サーバ 4 0 を防御することができず、さらに、W e b サーバ 4 0 からクライアント装置 1 0 に不正レスポンスが送信されるおそれがある。

【 0 1 7 3 】

そこで、本実施の形態 7 では、暗号処理がなされた H T T P リクエストを復号するとともに、暗号処理がなされたレスポンスを復号することによって、暗号化がなされた不正アクセスや暗号化がなされた不正レスポンスをも破棄することができるようにしている。以下、本実施の形態 7 に係るサーバクライアントシステムにおけるサーバ装置の構成を説明する。

【 0 1 7 4 】

図 1 3 は、本実施の形態 7 に係るサーバクライアントシステムの構成を示すブロック図である。なお、図 1 または図 1 1 に示した各部と同様の機能を有する部位には同一符号を付すこととしてその詳細な説明を省略し、本実施の形態 7 の特徴部分である復号部 1 2 2 および復号部 1 2 3 について説明する。

【 0 1 7 5 】

サーバ装置 1 2 0 におけるリクエストフィルタ 1 2 1 の復号部 1 2 2 は、所定の暗号処理がなされた HTTP リクエストを復号する復号手段である。具体的には、受信部 3 1 から暗号処理がなされた HTTP リクエストを受け取った後、この HTTP リクエストを復号し、復号した HTTP リクエストを見積部 3 2 に出力する。これによって、見積部 3 2 は、上記実施の形態 1 または 2 で説明した見積処理を実行することとなる。

【 0 1 7 6 】

なお、受信部 3 1 は、暗号処理がなされた HTTP リクエストを送信部 3 5 に出力するので、Web サーバ 4 0 には、暗号処理がなされた HTTP リクエストが送信されることとなる。これによって、一つのリクエストフィルタ 1 2 1 により複数の Web サーバ 4 0 を防御するために、リクエストフィルタ 1 2 1 と複数の Web サーバ 4 0 とをインターネットなどの非専用回線で接続した場合でも、HTTP リクエストの秘匿性を確保することができる。

【 0 1 7 7 】

一方、復号部 1 2 3 は、所定の暗号処理がなされたレスポンスを復号する第 2 の復号手段である。具体的には、レスポンス受信部 1 1 2 から暗号処理がなされたレスポンスを受け取った後、このレスポンスを復号し、復号したレスポンスをレスポンス見積部 1 1 3 に出力する。これによって、レスポンス見積部 1 1 3 は、上記実施の形態 6 で説明した見積処理を実行することとなる。

【 0 1 7 8 】

なお、レスポンス受信部 1 1 2 は、暗号処理がなされたレスポンスをレスポンス送信部 1 1 6 に出力するので、クライアント装置 1 0 には、暗号処理がなされたレスポンスが送信されることとなる。これによって、クライアント装置 1 0 に

送信されるレスポンスの秘匿性を確保することができる。

【0179】

上述してきたように、本実施の形態7によれば、暗号処理がなされたHTTPリクエストを復号するとともに、暗号処理がなされたレスポンスを復号することとしたので、クライアント装置10から暗号処理がなされたHTTPリクエストを受信するとともに、暗号処理がなされたレスポンスをクライアント装置10に送信するようにしたWebサーバ40に適用する場合においても、暗号化がなされた不正アクセスや暗号化がなされた不正レスポンスを破棄することができる。これによって、不正アクセスからWebサーバ40を確実に防御することができ、さらに、Webサーバ40からクライアント装置10に不正レスポンスが送信されるおそれを確実に排除することができる。

【0180】

なお、本実施の形態7では、HTTPリクエストおよびレスポンスを復号する場合を説明したが、本発明はこれに限定されるものではなく、HTTPリクエストのみを復号する場合や、レスポンスのみを復号する場合など、Webサーバ40の処理態様（暗号処理がなされたHTTPリクエストを受信するか否か、暗号処理がなされたレスポンスを送信するか否かなど）に応じて、HTTPリクエストまたはレスポンスの一方を復号する場合に同様に適用することができる。

【0181】

また、本実施の形態7では、リクエストフィルタ121によりHTTPリクエストを復号した後に、Webサーバ40には、暗号処理がなされたHTTPリクエストを送信する場合を説明したが、本発明はこれに限定されるものではなく、Webサーバ40に対して、復号されたHTTPリクエストを送信する場合にも同様に適用することができる。なお、この場合には、Webサーバ40の復号手段を省略することができる。

【0182】

また、本実施の形態7では、クライアント装置10から送信されたHTTPリクエストに対しては、パターンに基づくフィルタリング処理を実行する場合を説明したが、本発明はこれに限定されるものではなく、上記実施の形態3で説明し

た事前判定処理や、上記実施の形態４で説明した統計に基づくフィルタリング処理をともに実行する場合にも同様に適用することができる。なお、この場合にも、事前判定処理や統計に基づくフィルタリング処理に先だって、本実施の形態７で説明した復号処理が実行される。

【 0 1 8 3 】

(実施の形態 8)

ところで、上記実施の形態１～７では、不正なＨＴＴＰリクエストや不正なレスポンスを破棄する場合を説明したが、本発明はこれに限定されるものではなく、クライアント装置１０に対して、不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを送信することもできる。

【 0 1 8 4 】

すなわち、不正なＨＴＴＰリクエストや不正なレスポンスを破棄するだけでは、不正アクセスを試行した攻撃者（クラッカー）は、不正アクセスが失敗したことに気づいて、新たな別の不正アクセスを試行するおそれがある。このため、望ましくは、不正アクセスが失敗したことを攻撃者に気づかせることなく時間を稼ぐことによって、新たな別の不正アクセスを未然に防止したり、攻撃者の攻撃手口を解析することが必要とされる。

【 0 1 8 5 】

ところで、従来より、不正アクセスからサーバを保護する技術として、おとりシステム（おとりサーバ、ハニーポット）と呼ばれる技術が一般的に知られている。このおとりシステムは、セキュリティホールを有するといった脆弱なサーバを装って、攻撃者による不正アクセスの試行を全てロギングするものである。

【 0 1 8 6 】

すなわち、攻撃者は一般的に、ネットワーク上のセキュリティレベルの低いサーバを攻撃対象とする行動志向を有するので、おとりシステムは、脆弱なサーバを装って、攻撃者がおとりシステムにアクセスしたならば、真のサーバ（不正アクセスから保護したいサーバ）であるかのようにログインバナーの返信などをする。そして、攻撃者が辞書を用いたパスワードクラッキングなどによってログインを試行してきた場合には、これらの行動を全てログとして安全に記録する。

【 0 1 8 7 】

このようにして、おとりシステムは、真のサーバが攻撃されるまでの時間を稼ぎ、新たな別の不正アクセスを未然に防止したり、攻撃者の攻撃手口（攻撃に用いる辞書など）を解析する。そして、この攻撃手口の解析結果や時間稼ぎによって、真のサーバに対する防御策を講じることが可能になる。

【 0 1 8 8 】

しかしながら、おとりシステムは、不正アクセスから保護したい真のサーバのおとりにはなれないという問題点がある。すなわち、あるサーバを保護しようとする場合、一般的に、おとりシステムは、そのサーバのミラーサーバ若しくはテストサーバを装って（それらを連想させる名前を付与されて）運用される。これは、真のサーバに対して正規にアクセスしようとする正規ユーザのために、真のサーバについては、真のサーバとわかる名前を付与して運用しなければならないからである。

【 0 1 8 9 】

したがって、真のサーバを保護するために、おとりシステムを導入しても、攻撃者がおとりシステムに目もくれず、真のサーバを攻撃してきたような場合には、おとりシステムの機能は没却され、真のサーバを保護するという目的を達成することができなくなってしまう。

【 0 1 9 0 】

そこで、本実施の形態 8 では、おとりシステムではなく、Webサーバ 4 0 に対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納した偽レスポンスデータベースを導入することによって、不正アクセスを試行したクライアント装置 1 0 に対して、不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを送信することができるようになっている。以下、本実施の形態 8 に係るサーバクライアントシステムにおけるサーバ装置の構成と、本実施の形態 8 によるフィルタリングの処理手順とを説明する。

【 0 1 9 1 】

(1) サーバ装置の構成

まず最初に、本実施の形態 8 に係るサーバクライアントシステムにおけるサーバ装置の構成を説明する。図 1 4 は、本実施の形態 8 に係るサーバクライアントシステムの構成を示すブロック図である。同図に示すように、本実施の形態 8 におけるサーバ装置 1 3 0 は、Web サーバ 4 0 と、リクエストフィルタ 1 3 1 とを備え、さらに、このリクエストフィルタ 1 3 1 は、受信部 3 1 と、見積部 3 2 と、不正リクエスト DB 3 3 と、判定部 3 4 と、送信部 3 5 と、偽レスポンス作成部 1 3 2 と、偽レスポンス DB 1 3 3 と、レスポンス送信部 1 3 4 とを備える。

【0 1 9 2】

このうち、受信部 3 1、見積部 3 2、不正リクエスト DB 3 3、判定部 3 4 および送信部 3 5 は、図 1 に示した同一符号を付している各部と同様の機能を有し、上記実施の形態 1 または 2 に示したフィルタリング処理と同様の処理、すなわち、パターンに基づくフィルタリング処理を実行するものである。このフィルタリング処理によって、不正な HTTP リクエストは、Web サーバ 4 0 に送信されることなく、偽レスポンス作成部 1 3 2 に出力される。

【0 1 9 3】

偽レスポンス作成部 1 3 2 は、偽レスポンス DB 1 3 3 および所定の作成ルールに基づいて、不正アクセスとして Web サーバ 4 0 に受け渡されなかった HTTP リクエストのパターンに対応した偽のレスポンスを作成する処理部である。

【0 1 9 4】

ここで、上記の偽レスポンス DB 1 3 3 は、Web サーバ 4 0 に対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納したデータベースである。具体的には、不正リクエスト DB 3 3 に格納された不正アクセスのパターンに対応付けて偽のレスポンスを記憶する。例えば、Web サーバ 4 0 上のパスワードファイルをリクエストする不正アクセスのパターンに対応付けられた、架空の情報からなる偽のパスワードファイルや、Web サーバ 4 0 に不正にログインしようとする不正アクセスのパターンに対応付けられた、偽のログインバナーなどを記憶する。

【0 1 9 5】

そして、偽レスポンス作成部 1 3 2 は、このような情報を格納した偽レスポンス DB 1 3 3 を参照することにより、不正アクセスとして Web サーバ 4 0 に受け渡されなかった HTTP リクエストのパターンに対応した偽のレスポンスを作成する。

【 0 1 9 6 】

具体的には、Web サーバ 4 0 上のパスワードファイルをリクエストする HTTP リクエストが、不正アクセスとして偽レスポンス作成部 1 3 2 に入力された場合には、偽レスポンス DB 1 3 3 に格納された偽のパスワードファイルを用いて偽のレスポンスを作成する。また、Web サーバ 4 0 に不正にログインしようとする HTTP リクエストが、不正アクセスとして偽レスポンス作成部 1 3 2 に入力された場合には、偽レスポンス DB 1 3 3 に格納された偽のログインバナーを用いて偽のレスポンスを作成する。

【 0 1 9 7 】

レスポンス送信部 1 3 4 は、Web サーバ 4 0 により正当に作成された正当レスポンスや、偽レスポンス作成部 1 3 2 により作成された偽のレスポンスをクライアント装置 1 0 に送信する処理部である。なお、図 1 4 には図示していないが、本実施の形態 8 のリクエストフィルタ 1 3 1 は、図 1 に示した実施の形態 1 のリクエストフィルタ 3 0 と同様、ログ管理部、外部通信部、外部情報取得部および更新部を備えるものである。

【 0 1 9 8 】

(2) フィルタリング処理

次に、本実施の形態 8 によるフィルタリングの処理手順について説明する。図 1 5 は、本実施の形態 8 によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置 1 3 0 におけるリクエストフィルタ 1 3 1 の受信部 3 1 は、クライアント装置 1 0 からの HTTP リクエストを Web サーバ 4 0 が受信する前に受信する（ステップ S 1 5 0 1 ）。

【 0 1 9 9 】

続いて、リクエストフィルタ 1 3 1 は、この HTTP リクエストを見積部 3 2 に受け渡し、上記実施の形態 1 または 2 によるフィルタリング処理と同様の処理

、すなわち、パターンに基づくフィルタリング処理を実行する（ステップ S 1 5 0 2 ～ S 1 5 0 5、ステップ S 1 5 0 7 および S 1 5 0 8）。

【 0 2 0 0 】

すなわち、見積部 3 2 は、不正リクエスト DB 3 3 に格納されたサーバに対する不正アクセスのパターンに基づいて、HTTP リクエストの正当性を見積もり（ステップ S 1 5 0 2）、判定部 3 4 は、HTTP リクエストを Web サーバ 4 0 に受け渡すか否か（すなわち、正当リクエストである旨が見積もられたか否か、または見積値 DI が所定の閾値以下であるか否か）を判定する（ステップ S 1 5 0 3）。

【 0 2 0 1 】

この判定により、正当リクエストである旨が見積もられた場合には（ステップ S 1 5 0 3 肯定）、送信部 3 5 は、HTTP リクエストをプロセス間通信により Web サーバ 4 0 に送信し（ステップ S 1 5 0 4）、Web サーバ 4 0 は、HTTP リクエストに応じたレスポンスを作成するなど、正当判定時の処理をおこなう（ステップ S 1 5 0 5）。続いて、レスポンス送信部 1 3 4 は、Web サーバ 4 0 により作成されたレスポンスをクライアント装置 1 0 に送信する（ステップ S 1 5 0 6）

【 0 2 0 2 】

これとは反対に、HTTP リクエストを Web サーバ 4 0 に受け渡さないものと判定された場合（すなわち、不正リクエストである旨が見積もられた場合、または見積値 DI が所定の閾値以上である場合）には（ステップ S 1 5 0 3 否定）、送信部 3 5 は、HTTP リクエストの Web サーバ 4 0 への受け渡しを拒絶する（ステップ S 1 5 0 7）。さらに、リクエストフィルタ 1 3 1 の各部は、不正リクエストの破棄、格納媒体への格納、外部装置への通報などの不正判定時の処理をおこなう（ステップ S 1 5 0 8）。

【 0 2 0 3 】

続いて、偽レスポンス作成部 1 3 2 は、偽レスポンス DB 1 3 3 および所定の作成ルール 1 3 2 a に基づいて、不正アクセスとして Web サーバ 4 0 に受け渡されなかった HTTP リクエストのパターンに対応した偽のレスポンスを作成す

る（ステップ S 1 5 0 9）。具体的には、偽レスポンス DB 1 3 3 に格納された偽のパスワードファイルを用いた偽のレスポンスや、偽レスポンス DB 1 3 3 に格納された偽のログインバナーを用いた偽のレスポンスなどを作成する。その後、レスポンス送信部 1 3 4 は、偽レスポンス作成部 1 3 2 により作成された偽のレスポンスをクライアント装置 1 0 に送信する（ステップ S 1 5 1 0）。

【 0 2 0 4 】

上記した一連の処理によって、不正アクセスのパターンに該当する HTTP リクエストを Web サーバ 4 0 に送信してきたクライアント装置 1 0 に対して、不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを送信されることとなる。

【 0 2 0 5 】

上述してきたように、本実施の形態 8 によれば、Web サーバ 4 0 に対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納した偽レスポンス DB 1 3 3 を導入することとしたので、不正アクセスを試行したクライアント装置 1 0 に対して、不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを送信することができる。これによって、不正アクセスが失敗したことを攻撃者に気づかせることなく時間を稼ぐことができ、さらに、新たな別の不正アクセスを未然に防止したり、攻撃者の攻撃手口を解析することもできるので、クライアント装置 1 0 による不正アクセスから Web サーバ 4 0 を一層確実に防御することが可能になる。

【 0 2 0 6 】

なお、本実施の形態 8 では、クライアント装置 1 0 から送信された HTTP リクエストに対しては、パターンに基づくフィルタリング処理を実行する場合を説明したが、本発明はこれに限定されるものではなく、上記実施の形態 3 で説明した事前判定処理や、上記実施の形態 4 で説明した統計に基づくフィルタリング処理、さらには、上記実施の形態 6 で説明したレスポンスのフィルタリング処理とともに実行する場合にも同様に適用することができる。

【 0 2 0 7 】

すなわち、例えば、上記実施の形態 6 で説明したレスポンスのフィルタリング

処理をともに実行する場合には、偽レスポンスDB 1 3 3に、不正なレスポンスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンス（例えば、偽のディレクトリ情報など）を格納することとなる。

【 0 2 0 8 】

ただし、上記実施の形態4で説明した統計に基づくフィルタリング処理をともに実施する場合には、かかるフィルタリング処理により破棄されたHTTPレスポンスについては、偽レスポンスを作成しないようにすることも有効である。このようなサーバダウンを狙ったHTTPレスポンスに対して偽レスポンスを作成したのでは、偽レスポンス作成処理の負担が却って増大してしまうからである。

【 0 2 0 9 】

（実施の形態9）

ところで、上記実施の形態8では、Webサーバ40に対する不正アクセスのパターンに対応する偽のレスポンスを格納した偽レスポンスDB 1 3 3を参照して、偽レスポンスを作成する場合を説明したが、本発明はこれに限定されるものではなく、不正アクセスとしてWebサーバ40に受け渡されなかったHTTPリクエストを受け入れて、Webサーバ40のおとりとして機能する偽Webサーバによって、偽のレスポンスを作成することもできる。

【 0 2 1 0 】

すなわち、Webサーバ40に対する不正アクセスには、パターンとして把握できないものもあり、このような不正アクセスについては、上記実施の形態8で説明した偽レスポンスDB 1 3 3を参照して偽レスポンスを作成することできない。このため、不正アクセスが失敗したことを攻撃者に気づかせることなく時間を稼ぐこともできず、さらに、新たな別の不正アクセスを未然に防止したり、攻撃者の攻撃手口を解析することもできなくなってしまう。

【 0 2 1 1 】

そこで、本実施の形態9では、偽レスポンスDB 1 3 3ではなく、不正なアクセスとしてWebサーバ40に受け渡されなかったHTTPリクエストを受け入れて、Webサーバ40のおとりとして該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを作成する偽Webサーバを導入することによって

、パターンとして把握できない不正アクセスに対しても、偽のレスポンスを送信することができるようにしている。以下、本実施の形態 9 に係るサーバクライアントシステムにおけるサーバ装置の構成と、本実施の形態 9 によるフィルタリングの処理手順とを説明する。

【0212】

図 16 は、本実施の形態 9 に係るサーバクライアントシステムの構成を示すブロック図である。なお、図 14 に示した各部と同様の機能を有する部位には同一符号を付すこととしてその詳細な説明を省略し、本実施の形態 9 の特徴部分である偽 Web サーバ 142 について説明する。

【0213】

サーバ装置 140 におけるリクエストフィルタ 141 の偽 Web サーバ 142 は、不正なアクセスとして Web サーバ 40 に受け渡されなかった HTTP リクエストを受け入れて、Web サーバ 40 のおとりとして該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを作成する処理部である。具体的には、Web サーバ 40 と同様、HTTP リクエストに応じて HTML (HyperText Markup Language) などのマークアップ言語により記述された各種の情報を送信するなどのサービスをクライアント装置 10 に提供するものであるが、Web サーバ 40 のおとりとして、偽のサービスを提供（偽のレスポンスを作成）するように偽のデータを所有する。

【0214】

例えば、Web サーバ 40 上のパスワードファイルをリクエストする不正な HTTP リクエストを受け入れて、偽のパスワードファイルを作成したり、コマンド文字列を含んだリクエストにより Web サーバ 40 上で任意のシステムコマンドを実行するなどの不正な HTTP リクエストを受け入れて、そのシステムコマンドを実行したり、Web サーバ 40 上に存在しないファイルをリクエストして Web サーバ 40 の機能を停止させる不正な HTTP リクエストを受け入れて、その機能を停止させる処理などをおこなう。

【0215】

すなわち、偽 Web サーバ 142 は、不正な HTTP リクエストを受け入れて

、そのHTTPリクエストに応じた処理を実行するものであるが、Webサーバ40のおとりとして偽のデータを所有するものであるため、偽Webサーバ142からのレスポンスは、不正なHTTPリクエストを受け入れたWebサーバ40からのレスポンスと同様のものであるが、偽のレスポンスとなる。

【0216】

次に、本実施の形態9によるフィルタリングの処理手順について説明する。図17は、本実施の形態9によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置140におけるリクエストフィルタ141は、クライアント装置10からのHTTPリクエストをWebサーバ40が受信する前に受信して（ステップS1701）、上記実施の形態8によるフィルタリング処理と同様の処理（図15に示したステップS1501～S1508）を実行する（ステップS1701～ステップS1708）。

【0217】

このステップS1708に示すように、リクエストフィルタ141の各部は、不正リクエストの破棄、格納媒体への格納、外部装置への通報などの不正判定時の処理をおこなうと（ステップS1708）、続いて、送信部35は、不正アクセスとしてWebサーバ40に受け渡されなかったHTTPリクエストを、偽Webサーバ142に送信する（ステップS1709）。

【0218】

そして、偽Webサーバ142は、Webサーバ40のおとりとして該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを作成する（ステップS1710）。具体的には、Webサーバ40上のパスワードファイルをリクエストする不正なHTTPリクエストを受け入れて、偽のパスワードファイルを作成したり、コマンド文字列を含んだリクエストによりWebサーバ40上で任意のシステムコマンドを実行するなどの不正なHTTPリクエストを受け入れて、そのシステムコマンドを実行したりなどする。その後、レスポンス送信部134は、偽Webサーバ142により作成された偽のレスポンスをクライアント装置10に送信する（ステップS1711）。

【0219】

上記した一連の処理によって、不正アクセスのパターンとして把握できないHTTPリクエストをWebサーバ40に送信してきたクライアント装置10に対しても、不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを送信されることとなる。

【0220】

上述してきたように、本実施の形態9によれば、不正なアクセスとしてWebサーバ40に受け渡されなかったHTTPリクエストを受け入れて、Webサーバ40のおとりとして該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを作成する偽Webサーバ142を導入することとしたので、パターンとして把握できない不正アクセスに対しても、偽のレスポンスを送信することができる。特に、上記実施の形態8で説明したおとりシステムと異なり、偽Webサーバ142は、不正アクセスから保護したいWebサーバ40のミラーサーバ若しくはテストサーバを装って運用される必要がないので、実質的にWebサーバ40のおとりになれる点でも有効であると考えられる。

【0221】

なお、本実施の形態9においても、クライアント装置10から送信されたHTTPリクエストに対しては、パターンに基づくフィルタリング処理を実行する場合を説明したが、本発明はこれに限定されるものではなく、上記実施の形態8と同様、上記実施の形態3で説明した事前判定処理や、上記実施の形態4で説明した統計に基づくフィルタリング処理、さらには、上記実施の形態6で説明したレスポンスのフィルタリング処理をともに実行する場合にも同様に適用することができる。

【0222】

(実施の形態10)

ところで、上記実施の形態8および9では、Webサーバ40に受け渡されなかった不正なHTTPリクエストのパターンに対応した偽のレスポンスを作成する場合と、不正なHTTPリクエストを受け入れて、Webサーバ40のおとりとして偽のレスポンスを作成する場合とを説明したが、本発明はこれに限定されるものではなく、これらの両者をともに実行する場合にも同様に適用することが

できる。

【0223】

すなわち、上記実施の形態9では、Webサーバ40に受け渡されなかった不正なHTTPリクエストの全てを偽Webサーバ142に受け渡すことによって、偽のレスポンスを作成することとしたが、不正アクセスのパターンとして把握できる不正なHTTPリクエストについても偽Webサーバ142に受け渡したのでは、偽Webサーバ142に過度な負担が強えられることとなる。

【0224】

そこで、本実施の形態10では、不正アクセスのパターンとして把握できる不正なHTTPリクエストについては、不正レスポンスDB133を参照して偽レスポンスを作成する一方、不正アクセスのパターンとして把握できない不正なHTTPリクエストについては、偽Webサーバ142により偽レスポンスを作成することとし、偽レスポンスを効率的かつ迅速に作成することができるようにしている。以下、本実施の形態10に係るサーバクライアントシステムにおけるサーバ装置の構成と、本実施の形態10によるフィルタリングの処理手順とを説明する。

【0225】

図18は、本実施の形態10に係るサーバクライアントシステムの構成を示すブロック図である。なお、図14または16に示した各部と同様の機能を有する部位には同一符号を付すこととしてその詳細な説明を省略し、本実施の形態10の特徴部分である偽レスポンス作成部152について説明する。

【0226】

サーバ装置150におけるリクエストフィルタ151の偽レスポンス作成部152は、偽レスポンスDB133および所定の作成ルール152aに基づいて、不正アクセスとしてWebサーバ40に受け渡されなかったHTTPリクエストのパターンに対応した偽のレスポンスを作成するとともに、偽のレスポンスが作成できなかったHTTPリクエストを偽Webサーバ142に受け渡す処理部である。

【0227】

具体的には、偽レスポンス作成部 1 5 2 は、不正アクセスとして Web サーバ 4 0 に受け渡されなかった HTTP リクエストを送信部 3 5 から受け付け、この HTTP リクエストのパターンが偽レスポンス DB 1 3 3 に格納されている不正リクエストのパターンに該当するか否かを判定する。そして、このパターンに該当する場合には、上記実施の形態 8 と同様、偽レスポンス DB 1 3 3 に基づいて偽レスポンスを作成する。一方、このパターンに該当しない場合には、HTTP リクエストを偽 Web サーバ 1 4 2 に受け渡し、偽 Web サーバ 1 4 2 に、上記実施の形態 9 の同様、Web サーバ 4 0 のおとりとして偽レスポンスを作成させる。

【 0 2 2 8 】

次に、本実施の形態 1 0 によるフィルタリングの処理手順について説明する。図 1 9 は、本実施の形態 1 0 によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置 1 5 0 におけるリクエストフィルタ 1 5 1 は、クライアント装置 1 0 からの HTTP リクエストを Web サーバ 4 0 が受信する前に受信して（ステップ S 1 9 0 1）、上記実施の形態 8 によるフィルタリング処理と同様の処理（図 1 5 に示したステップ S 1 5 0 1 ～ S 1 5 0 8）を実行する（ステップ S 1 9 0 1 ～ ステップ S 1 9 0 8）。

【 0 2 2 9 】

このステップ S 1 9 0 8 に示すように、リクエストフィルタ 1 5 1 の各部は、不正リクエストの破棄、格納媒体への格納、外部装置への通報などの不正判定時の処理をおこなうと（ステップ S 1 9 0 8）、続いて、偽レスポンス作成部 1 5 2 は、破棄された HTTP リクエストのパターンが偽レスポンス DB 1 3 3 に格納されている不正リクエストのパターンに該当するか否かを判定する（ステップ S 1 9 0 9）。

【 0 2 3 0 】

この判定により、不正リクエストのパターンに該当する場合には（ステップ S 1 9 0 9 肯定）、偽レスポンス作成部 1 5 2 は、偽レスポンス DB 1 3 3 および所定の作成ルール 1 5 2 a に基づいて、不正アクセスとして Web サーバ 4 0 に受け渡されなかった HTTP リクエストのパターンに対応した偽のレスポンスを

作成する（ステップ S 1 9 1 0）。そして、レスポンス送信部 1 3 4 は、偽レスポンス作成部 1 5 2 により作成された偽のレスポンスをクライアント装置 1 0 に送信する（ステップ S 1 9 1 1）。

【0 2 3 1】

これとは反対に、不正リクエストのパターンに該当しない場合には（ステップ S 1 9 0 9 否定）偽レスポンス作成部 1 5 2 は、パターンに該当しなかった H T T P リクエストを偽 W e b サーバ 1 4 2 に送信する（ステップ S 1 9 1 2）。そして、偽 W e b サーバ 1 4 2 は、W e b サーバ 4 0 のおとりとして該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを作成する（ステップ S 1 9 1 3）。その後、レスポンス送信部 1 3 4 は、偽 W e b サーバ 1 4 2 により作成された偽のレスポンスをクライアント装置 1 0 に送信する（ステップ S 1 9 1 1）。

【0 2 3 2】

上記した一連の処理によって、不正アクセスのパターンとして把握できる不正な H T T P リクエストについては、不正レスポンス D B 1 3 3 を参照して偽レスポンスが作成される一方、不正アクセスのパターンとして把握できない不正な H T T P リクエストについては、偽 W e b サーバ 1 4 2 により偽レスポンスが作成されることとなる。

【0 2 3 3】

上述してきたように、本実施の形態 1 0 によれば、不正アクセスのパターンとして把握できる不正な H T T P リクエストについては、不正レスポンス D B 1 3 3 を参照して偽レスポンスを作成する一方、不正アクセスのパターンとして把握できない不正な H T T P リクエストについては、偽 W e b サーバ 1 4 2 により偽レスポンスを作成することとしたので、偽 W e b サーバ 1 4 2 に過度な負担を強いることなく、偽レスポンスを効率的かつ迅速に作成することができる。

【0 2 3 4】

なお、本実施の形態 1 0 においても、クライアント装置 1 0 から送信された H T T P リクエストに対しては、パターンに基づくフィルタリング処理を実行する場合を説明したが、本発明はこれに限定されるものではなく、上記実施の形態 8

および 9 と同様、上記実施の形態 3 で説明した事前判定処理や、上記実施の形態 4 で説明した統計に基づくフィルタリング処理、さらには、上記実施の形態 6 で説明したレスポンスのフィルタリング処理をともに実行する場合にも同様に適用することができる。

【 0 2 3 5 】

(他の実施の形態)

さて、これまで本発明の実施の形態について説明したが、本発明は上述した実施の形態以外にも、上記特許請求の範囲に記載した技術的思想の範囲内において種々の異なる実施の形態にて実施されてもよいものである。

【 0 2 3 6 】

例えば、本実施の形態 4 ～ 1 0 では、クライアント装置 1 0 からの HTTP リクエストをフィルタリングする場合について説明したが、本発明はこれに限定されるものではなく、FTP (File Transfer Protocol)、telnet、コンソールなど、クライアント装置 1 0 から Web サーバ 4 0 に入力されるあらゆる情報をフィルタリングする場合に同様に適用することができる。

【 0 2 3 7 】

また、本実施の形態 4 ～ 1 0 では、フィルタリング装置としてのリクエストフィルタをサーバ装置に設けた場合について説明したが、本発明はこれに限定されるものではなく、例えば、それぞれのクライアント装置側にリクエストフィルタを設けたり、一つのリクエストフィルタにより複数の Web サーバを防御するなど、クライアント装置と Web サーバとの間にリクエストフィルタが介在するあらゆるシステム構成において同様に適用することができる。

【 0 2 3 8 】

なお、本実施の形態 4 ～ 1 0 で説明したフィルタリング方法は、あらかじめ用意されたプログラムをパーソナル・コンピュータやワークステーションなどのコンピュータで実行することによって実現することができる。このプログラムは、インターネットなどのネットワークを介して配布することができる。また、このプログラムは、ハードディスク、フレキシブルディスク (FD)、CD-ROM、MO、DVD などのコンピュータで読み取り可能な記録媒体に記録され、コン

ピュータによって記録媒体から読み出されることによって実行することもできる。

【 0 2 3 9 】

（付記 1）クライアントと該クライアントからのアクセス要求に応じてサービスを提供するサーバとの間に介在し、前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡すフィルタリング装置において、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースと、

前記不正パターンデータベースに格納された不正アクセスのパターンおよび所定の第 1 の見積ルールに基づいて前記アクセス要求の正当性を見積もる第 1 の見積手段と、

前記第 1 の見積手段による見積結果および所定の第 1 の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する第 1 の判定手段と、

を備えたことを特徴とするフィルタリング装置。

【 0 2 4 0 】

（付記 2）前記第 1 の見積手段は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第 1 の判定手段は、前記第 1 の見積手段により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第 1 の見積手段により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記 1 に記載のフィルタリング装置。

【 0 2 4 1 】

（付記 3）前記第 1 の見積手段は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、前記第 1 の判定手段は、前記第 1 の見積手段により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを

判定することを特徴とする付記 1 に記載のフィルタリング装置。

【 0 2 4 2 】

(付記 4) 前記サーバに対する正当アクセスのパターンを格納した正当パターンデータベースと、前記第 1 の見積手段による正当性を見積もりの前に、前記アクセス要求が前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定する事前判定手段と、をさらに備え、前記第 1 の見積手段は、前記事前判定手段により正当アクセスのパターンに該当しないものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記 1、2 または 3 に記載のフィルタリング装置。

【 0 2 4 3 】

(付記 5) 所定の第 1 の外部送信ルールに基づいて、前記第 1 の判定手段により前記サーバに受け渡さないものと判定されたアクセス要求を所定の外部装置に送信する第 1 の外部送信手段をさらに備えたことを特徴とする付記 1 ～ 4 のいずれか一つに記載のフィルタリング装置。

【 0 2 4 4 】

(付記 6) 所定の第 1 の格納ルールに基づいて、前記第 1 の判定手段により前記サーバに受け渡さないものと判定されたアクセス要求を所定の格納媒体に格納する第 1 の格納手段をさらに備えたことを特徴とする付記 1 ～ 5 のいずれか一つに記載のフィルタリング装置。

【 0 2 4 5 】

(付記 7) 所定の第 1 の更新ルールに基づいて、前記不正パターンデータベース、正当パターンデータベース、第 1 の見積ルール、第 1 の判定ルール、第 1 の外部送信ルール、第 1 の格納ルールまたは第 1 の更新ルールを更新する第 1 の更新手段をさらに備えたことを特徴とする付記 1 ～ 6 のいずれか一つに記載のフィルタリング装置。

【 0 2 4 6 】

(付記 8) 前記サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求に関する情報を格納した統計的不正データベースと、前記統計的不正データベースに格納された情報および所定の第 2 の見積ルールに基づい

て前記アクセス要求の正当性を見積もる第 2 の見積手段と、前記見積手段による見積結果および所定の第 2 の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する第 2 の判定手段と、前記第 1 および第 2 の判定手段により前記サーバに受け渡すものと判定されたアクセス要求のみを正当なアクセス要求として前記サーバに受け渡すアクセス要求受渡手段と、をさらに備えたことを特徴とする付記 1 ～ 7 のいずれか一つに記載のフィルタリング装置。

【 0 2 4 7 】

（付記 9）前記統計的不正データベースは、前記サーバに対してアクセス要求を送信したクライアントのうち、所定時間内のアクセス要求数が所定数を超えたクライアントの送信元情報を格納するものであって、

前記第 2 の見積手段は、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第 2 の判定手段は、前記第 2 の見積手段により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第 2 の見積手段により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記 8 に記載のフィルタリング装置。

【 0 2 4 8 】

（付記 1 0）前記統計的不正データベースは、前記サーバに対して送信されたアクセス要求の要求内容のうち、所定時間内のアクセス要求数が所定数を超えた要求内容を格納するものであって、

前記第 2 の見積手段は、前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第 2 の判定手段は、前記第 2 の見積手段により不正アクセスである旨が見積もられたアクセス要求を前記サー

バに受け渡さないものと判定するとともに、前記第2の見積手段により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記8に記載のフィルタリング装置。

【0249】

(付記11) 前記統計的不正データベースは、前記サーバに対してアクセス要求を送信したクライアントのうち、所定時間内のアクセス要求数が所定数を超えたクライアントの送信元情報を格納するとともに、前記サーバに対して送信されたアクセス要求の要求内容のうち、所定時間内のアクセス要求数が所定数を超えた要求内容を格納するものであって、

前記第2の見積手段は、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれかに該当する場合または前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれにも該当しない場合および前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれかにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第2の判定手段は、前記第2の見積手段により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第2の見積手段により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記8に記載のフィルタリング装置。

【0250】

(付記12) 前記統計的不正データベースは、前記サーバに対してアクセス要求を送信したクライアントのうち、所定時間内のアクセス要求数が所定数を超えたクライアントの送信元情報を格納するとともに、前記サーバに対して送信されたアクセス要求の要求内容のうち、所定時間内のアクセス要求数が所定数を超えた要求内容を格納するものであって、

前記第2の見積手段は、前記アクセス要求の送信元情報および要求内容が前記統計的不正データベースに格納された送信元情報および要求内容に該当する度合

に応じて所定の見積値を算出し、前記第 2 の判定手段は、前記第 2 の見積手段により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを判定することを特徴とする付記 8 に記載のフィルタリング装置。

【 0 2 5 1 】

(付記 1 3) 前記第 2 の見積手段は、前記第 1 の判定手段により前記サーバに受け渡すものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記 8 ～ 1 2 のいずれか一つに記載のフィルタリング装置。

【 0 2 5 2 】

(付記 1 4) 前記第 1 の見積手段は、前記第 2 の判定手段により前記サーバに受け渡すものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記 8 ～ 1 2 のいずれか一つに記載のフィルタリング装置。

【 0 2 5 3 】

(付記 1 5) 前記事前判定手段は、前記第 2 の判定手段により前記サーバに受け渡すものと判定されたアクセス要求のみについて前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定することを特徴とする付記 8 ～ 1 2 のいずれか一つに記載のフィルタリング装置。

【 0 2 5 4 】

(付記 1 6) 所定の第 2 の外部送信ルールに基づいて、前記アクセス要求受渡手段により前記サーバに受け渡されなかったアクセス要求を所定の外部装置に送信する第 2 の外部送信手段をさらに備えたことを特徴とする付記 8 ～ 1 5 のいずれか一つに記載のフィルタリング装置。

【 0 2 5 5 】

(付記 1 7) 所定の第 2 の格納ルールに基づいて、前記アクセス要求受渡手段により前記サーバに受け渡されなかったアクセス要求を所定の格納媒体に格納する第 2 の格納手段をさらに備えたことを特徴とする付記 8 ～ 1 6 のいずれか一つに記載のフィルタリング装置。

【 0 2 5 6 】

(付記 1 8) 所定の第 2 の更新ルールおよび／または前記サーバに対するアクセ

ス要求の統計に基づいて、前記統計的不正データベース、第2の見積ルール、第2の判定ルール、第2の外部送信ルール、第2の格納ルールおよび／または第2の更新ルールを更新する第2の更新手段をさらに備えたことを特徴とする付記8～17のいずれか一つに記載のフィルタリング装置。

【0257】

(付記19) 前記第2の更新手段は、所定時間内に前記サーバに対してアクセス要求を送信した各クライアントごとのアクセス要求数および／または所定時間内に前記サーバに対して送信されたアクセス要求の各要求内容ごとのアクセス要求数に応じて、前記統計的不正データベースに格納される送信元情報および／または要求内容を追加および／または削除することを特徴とする付記18に記載のフィルタリング装置。

【0258】

(付記20) 前記アクセス要求に応じて前記サーバから前記クライアントに対して前記サービスとして送信されるレスポンスのうち、前記クライアントに対して送信されるべきでない不正レスポンスのパターンを格納した不正レスポンスデータベースと、前記不正レスポンスデータベースに格納された不正レスポンスのパターンおよび所定のレスポンス見積ルールに基づいて前記レスポンスの正当性を見積もるレスポンス見積手段と、前記レスポンス見積手段による見積結果および所定のレスポンス判定ルールに基づいて前記レスポンスを前記クライアントに送信するか否かを判定するレスポンス判定手段と、前記レスポンス判定手段により前記クライアントに送信するものと判定されたレスポンスのみを正当なレスポンスとして前記クライアントに送信するレスポンス送信手段と、をさらに備えたことを特徴とする付記1～19のいずれか一つに記載のフィルタリング装置。

【0259】

(付記21) 前記レスポンス見積手段は、前記レスポンスが前記不正レスポンスデータベースに格納された不正レスポンスのパターンのいずれかに該当する場合に該レスポンスは不正レスポンスである旨を見積もるとともに、前記レスポンスが前記不正レスポンスデータベースに格納された不正レスポンスのパターンのいずれにも該当しない場合に該レスポンスは正当レスポンスである旨を見積もり、

前記レスポンス判定手段は、前記レスポンス見積手段により不正レスポンスである旨が見積もられたレスポンスを前記クライアントに送信しないものと判定するとともに、前記レスポンス見積手段により正当レスポンスである旨が見積もられたレスポンスを前記クライアントに送信するものと判定することを特徴とする付記 2 0 に記載のフィルタリング装置。

【 0 2 6 0 】

（付記 2 2）前記レスポンス見積手段は、前記レスポンスが前記不正レスポンスデータベースに格納された不正レスポンスのパターンに該当する度合に応じて所定の見積値を算出し、前記レスポンス判定手段は、前記レスポンス見積手段により算出された見積値と所定の閾値とを比較して前記レスポンスを前記クライアントに送信するか否かを判定することを特徴とする付記 2 0 に記載のフィルタリング装置。

【 0 2 6 1 】

（付記 2 3）所定の第 3 の外部送信ルールに基づいて、前記レスポンス送信手段により前記クライアントに送信されなかったレスポンスおよび／または該レスポンスの起因となったアクセス要求を所定の外部装置に送信する第 3 の外部送信手段をさらに備えたことを特徴とする付記 2 0、2 1 または 2 2 に記載のフィルタリング装置。

【 0 2 6 2 】

（付記 2 4）所定の第 3 の格納ルールに基づいて、前記レスポンス送信手段により前記クライアントに送信されなかったレスポンスおよび／または該レスポンスの起因となったアクセス要求を所定の格納媒体に格納する第 3 の格納手段をさらに備えたことを特徴とする付記 2 0 ～ 2 3 のいずれか一つに記載のフィルタリング装置。

【 0 2 6 3 】

（付記 2 5）所定の第 3 の更新ルールに基づいて、前記不正レスポンスデータベース、レスポンス見積ルール、レスポンス判定ルール、第 3 の外部送信ルール、第 3 の格納ルールおよび／または第 3 の更新ルールを更新する第 3 の更新手段をさらに備えたことを特徴とする付記 2 0 ～ 2 4 のいずれか一つに記載のフィルタ

リング装置。

【 0 2 6 4 】

（付記 2 6）所定の暗号処理がなされたアクセス要求を復号する第 1 の復号手段をさらに備え、前記第 1 の見積手段、事前判定手段または第 2 の見積手段は、前記第 1 の復号手段により復号されたアクセス要求について見積または判定をおこなうことを特徴とする付記 1 ～ 2 5 のいずれか一つに記載のフィルタリング装置。

【 0 2 6 5 】

（付記 2 7）前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡す場合に、前記第 1 の復号手段により復号されたアクセス要求ではなく、所定の暗号処理がなされたアクセス要求を前記サーバに受け渡すことを特徴とする付記 2 6 に記載のフィルタリング装置。

【 0 2 6 6 】

（付記 2 8）所定の暗号処理がなされたレスポンスを復号する第 2 の復号手段をさらに備え、前記レスポンス見積手段は、前記第 2 の復号手段により復号されたレスポンスについて見積をおこなうことを特徴とする付記 2 6 または 2 7 に記載のフィルタリング装置。

【 0 2 6 7 】

（付記 2 9）前記レスポンスのうちの正当なレスポンスのみを前記クライアントに送信する場合に、前記第 2 の復号手段により復号されたレスポンスではなく、所定の暗号処理がなされたレスポンスを前記クライアントに送信することを特徴とする付記 2 8 に記載のフィルタリング装置。

【 0 2 6 8 】

（付記 3 0）前記サーバに対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納した偽レスポンスデータベースと、前記偽レスポンスデータベースを参照して、不正アクセスとして前記サーバに受け渡されなかったアクセス要求のパターンに対応した偽のレスポンスを作成する偽レスポンス作成手段と、前記偽レスポンス作成手段により作成された偽のレスポンスを前記クライアントに送信する偽レスポンス送信

手段と、をさらに備えたことを特徴とする付記 1 ～ 2 9 のいずれか一つに記載のフィルタリング装置。

【 0 2 6 9 】

（付記 3 1）不正なアクセスとして前記サーバに受け渡されなかったアクセス要求を受け入れて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを前記サーバのおとりとして作成するおとり手段と、前記おとり手段により作成された偽のレスポンスを前記クライアントに送信する偽レスポンス送信手段と、をさらに備えたことを特徴とする付記 1 ～ 2 9 のいずれか一つに記載のフィルタリング装置。

【 0 2 7 0 】

（付記 3 2）前記サーバに対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納した偽レスポンスデータベースと、不正アクセスとして前記サーバに受け渡されなかったアクセス要求のうち、前記偽レスポンスデータベースに格納された不正アクセスのパターンに対応するアクセス要求について該パターンに対応した偽のレスポンスを作成する偽レスポンス作成手段と、不正アクセスとして前記サーバに受け渡されなかったアクセス要求のうち、前記偽レスポンスデータベースに格納された不正アクセスのパターンに対応しないアクセス要求を受け入れて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを前記サーバのおとりとして作成するおとり手段と、前記偽レスポンス作成手段または前記おとり手段により作成された偽のレスポンスを前記クライアントに送信する偽レスポンス送信手段と、をさらに備えたことを特徴とする付記 1 ～ 2 9 のいずれか一つに記載のフィルタリング装置。

【 0 2 7 1 】

（付記 3 3）クライアントと該クライアントからのアクセス要求に応じてサービスを提供するサーバとの間に介在し、前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡すフィルタリング方法において、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースを参照し、該参照した不正アクセスのパターンおよび所定の第 1 の見積ルー

ルに基づいて前記アクセス要求の正当性を見積もる第 1 の見積工程と、

前記第 1 の見積工程による見積結果および所定の第 1 の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する第 1 の判定工程と、
を含んだことを特徴とするフィルタリング方法。

【 0 2 7 2 】

(付記 3 4) 前記第 1 の見積工程は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第 1 の判定工程は、前記第 1 の見積工程により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第 1 の見積工程により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記 3 3 に記載のフィルタリング方法。

【 0 2 7 3 】

(付記 3 5) 前記第 1 の見積工程は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、前記第 1 の判定工程は、前記第 1 の見積工程により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを判定することを特徴とする付記 3 3 に記載のフィルタリング方法。

【 0 2 7 4 】

(付記 3 6) 前記第 1 の見積工程による正当性を見積もりの前に、前記サーバに対する正当アクセスのパターンを格納した正当パターンデータベースを参照し、前記アクセス要求が前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定する事前判定工程をさらに含み、前記第 1 の見積工程は、前記事前判定工程により正当アクセスのパターンに該当しないものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記 3 3、3 4 または 3 5 に記載のフィルタリング方法。

【 0 2 7 5 】

（付記 3 7）所定の第 1 の外部送信ルールに基づいて、前記第 1 の判定工程により前記サーバに受け渡さないものと判定されたアクセス要求を所定の外部装置に送信する第 1 の外部送信工程をさらに含んだことを特徴とする付記 3 3 ～ 3 6 のいずれか一つに記載のフィルタリング方法。

【 0 2 7 6 】

（付記 3 8）所定の第 1 の格納ルールに基づいて、前記第 1 の判定工程により前記サーバに受け渡さないものと判定されたアクセス要求を所定の格納媒体に格納する第 1 の格納工程をさらに含んだことを特徴とする付記 3 3 ～ 3 7 のいずれか一つに記載のフィルタリング方法。

【 0 2 7 7 】

（付記 3 9）所定の第 1 の更新ルールに基づいて、前記不正パターンデータベース、正当パターンデータベース、第 1 の見積ルール、第 1 の判定ルール、第 1 の外部送信ルール、第 1 の格納ルールまたは第 1 の更新ルールを更新する第 1 の更新工程をさらに含んだことを特徴とする付記 3 3 ～ 3 8 のいずれか一つに記載のフィルタリング方法。

【 0 2 7 8 】

（付記 4 0）前記サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求に関する情報を格納した統計的不正データベースを参照し、所定の第 2 の見積ルールに基づいて前記アクセス要求の正当性を見積もる第 2 の見積工程と、前記見積工程による見積結果および所定の第 2 の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する第 2 の判定工程と、前記第 1 および第 2 の判定工程により前記サーバに受け渡すものと判定されたアクセス要求のみを正当なアクセス要求として前記サーバに受け渡すアクセス要求受渡工程と、をさらに含んだことを特徴とする付記 3 3 ～ 3 9 のいずれか一つに記載のフィルタリング方法。

【 0 2 7 9 】

（付記 4 1）前記統計的不正データベースは、前記サーバに対してアクセス要求を送信したクライアントのうち、所定時間内のアクセス要求数が所定数を超えた

クライアントの送信元情報を格納するものであって、

前記第 2 の見積工程は、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第 2 の判定工程は、前記第 2 の見積工程により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第 2 の見積工程により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記 4 0 に記載のフィルタリング方法。

【 0 2 8 0 】

(付記 4 2) 前記統計的不正データベースは、前記サーバに対して送信されたアクセス要求の要求内容のうち、所定時間内のアクセス要求数が所定数を越えた要求内容を格納するものであって、

前記第 2 の見積工程は、前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第 2 の判定工程は、前記第 2 の見積工程により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第 2 の見積工程により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記 4 0 に記載のフィルタリング方法。

【 0 2 8 1 】

(付記 4 3) 前記統計的不正データベースは、前記サーバに対してアクセス要求を送信したクライアントのうち、所定時間内のアクセス要求数が所定数を越えたクライアントの送信元情報を格納するとともに、前記サーバに対して送信されたアクセス要求の要求内容のうち、所定時間内のアクセス要求数が所定数を越えた要求内容を格納するものであって、

前記第 2 の見積工程は、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれかに該当する場合または前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれにも該当しない場合および前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれかにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第 2 の判定工程は、前記第 2 の見積工程により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第 2 の見積工程により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記 4 0 に記載のフィルタリング方法。

【 0 2 8 2 】

（付記 4 4）前記統計的不正データベースは、前記サーバに対してアクセス要求を送信したクライアントのうち、所定時間内のアクセス要求数が所定数を超えたクライアントの送信元情報を格納するとともに、前記サーバに対して送信されたアクセス要求の要求内容のうち、所定時間内のアクセス要求数が所定数を超えた要求内容を格納するものであって、

前記第 2 の見積工程は、前記アクセス要求の送信元情報および要求内容が前記統計的不正データベースに格納された送信元情報および要求内容に該当する度合に応じて所定の見積値を算出し、前記第 2 の判定工程は、前記第 2 の見積工程により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを判定することを特徴とする付記 4 0 に記載のフィルタリング方法。

【 0 2 8 3 】

（付記 4 5）前記第 2 の見積工程は、前記第 1 の判定工程により前記サーバに受け渡すものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記 4 0 ～ 4 4 のいずれか一つに記載のフィルタリング方法。

【 0 2 8 4 】

（付記 4 6）前記第 1 の見積工程は、前記第 2 の判定工程により前記サーバに受け渡すものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記 4 0 ～ 4 4 のいずれか一つに記載のフィルタリング方法。

【 0 2 8 5 】

（付記 4 7）前記事前判定工程は、前記第 2 の判定工程により前記サーバに受け渡すものと判定されたアクセス要求のみについて前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定することを特徴とする付記 4 0 ～ 4 4 のいずれか一つに記載のフィルタリング方法。

【 0 2 8 6 】

（付記 4 8）所定の第 2 の外部送信ルールに基づいて、前記アクセス要求受渡工程により前記サーバに受け渡されなかったアクセス要求を所定の外部装置に送信する第 2 の外部送信工程をさらに含んだことを特徴とする付記 4 0 ～ 4 7 のいずれか一つに記載のフィルタリング方法。

【 0 2 8 7 】

（付記 4 9）所定の第 2 の格納ルールに基づいて、前記アクセス要求受渡工程により前記サーバに受け渡されなかったアクセス要求を所定の格納媒体に格納する第 2 の格納工程をさらに含んだことを特徴とする付記 4 0 ～ 4 8 のいずれか一つに記載のフィルタリング方法。

【 0 2 8 8 】

（付記 5 0）所定の第 2 の更新ルールおよび／または前記サーバに対するアクセス要求の統計に基づいて、前記統計的不正データベース、第 2 の見積ルール、第 2 の判定ルール、第 2 の外部送信ルール、第 2 の格納ルールおよび／または第 2 の更新ルールを更新する第 2 の更新工程をさらに含んだことを特徴とする付記 4 0 ～ 4 9 のいずれか一つに記載のフィルタリング方法。

【 0 2 8 9 】

（付記 5 1）前記第 2 の更新工程は、所定時間内に前記サーバに対してアクセス要求を送信した各クライアントごとのアクセス要求数および／または所定時間内に前記サーバに対して送信されたアクセス要求の各要求内容ごとのアクセス要求数に応じて、前記統計的不正データベースに格納される送信元情報および／また

は要求内容を追加および／または削除することを特徴とする付記 5 0 に記載のフィルタリング方法。

【 0 2 9 0 】

（付記 5 2）前記アクセス要求に応じて前記サーバから前記クライアントに対して前記サービスとして送信されるレスポンスのうち、前記クライアントに対して送信されるべきでない不正レスポンスのパターンを格納した不正レスポンスデータベースを参照し、所定のレスポンス見積ルールに基づいて前記レスポンスの正当性を見積もるレスポンス見積工程と、前記レスポンス見積工程による見積結果および所定のレスポンス判定ルールに基づいて前記レスポンスを前記クライアントに送信するか否かを判定するレスポンス判定工程と、前記レスポンス判定工程により前記クライアントに送信するものと判定されたレスポンスのみを正当なレスポンスとして前記クライアントに送信するレスポンス送信工程と、をさらに含んだことを特徴とする付記 3 3 ～ 5 1 のいずれか一つに記載のフィルタリング方法。

【 0 2 9 1 】

（付記 5 3）前記レスポンス見積工程は、前記レスポンスが前記不正レスポンスデータベースに格納された不正レスポンスのパターンのいずれかに該当する場合に該レスポンスは不正レスポンスである旨を見積もるとともに、前記レスポンスが前記不正レスポンスデータベースに格納された不正レスポンスのパターンのいずれにも該当しない場合に該レスポンスは正当レスポンスである旨を見積もり、前記レスポンス判定工程は、前記レスポンス見積工程により不正レスポンスである旨が見積もられたレスポンスを前記クライアントに送信しないものと判定するとともに、前記レスポンス見積工程により正当レスポンスである旨が見積もられたレスポンスを前記クライアントに送信するものと判定することを特徴とする付記 5 2 に記載のフィルタリング方法。

【 0 2 9 2 】

（付記 5 4）前記レスポンス見積工程は、前記レスポンスが前記不正レスポンスデータベースに格納された不正レスポンスのパターンに該当する度合に応じて所定の見積値を算出し、前記レスポンス判定工程は、前記レスポンス見積工程によ

り算出された見積値と所定の閾値とを比較して前記レスポンスを前記クライアントに送信するか否かを判定することを特徴とする付記 5 2 に記載のフィルタリング方法。

【 0 2 9 3 】

(付記 5 5) 所定の第 3 の外部送信ルールに基づいて、前記レスポンス送信工程により前記クライアントに送信されなかったレスポンスおよび／または該レスポンスの起因となったアクセス要求を所定の外部装置に送信する第 3 の外部送信工程をさらに含んだことを特徴とする付記 5 2、5 3 または 5 4 に記載のフィルタリング方法。

【 0 2 9 4 】

(付記 5 6) 所定の第 3 の格納ルールに基づいて、前記レスポンス送信工程により前記クライアントに送信されなかったレスポンスおよび／または該レスポンスの起因となったアクセス要求を所定の格納媒体に格納する第 3 の格納工程をさらに含んだことを特徴とする付記 5 2 ～ 5 5 のいずれか一つに記載のフィルタリング方法。

【 0 2 9 5 】

(付記 5 7) 所定の第 3 の更新ルールに基づいて、前記不正レスポンスデータベース、レスポンス見積ルール、レスポンス判定ルール、第 3 の外部送信ルール、第 3 の格納ルールおよび／または第 3 の更新ルールを更新する第 3 の更新工程をさらに含んだことを特徴とする付記 5 2 ～ 5 6 のいずれか一つに記載のフィルタリング方法。

【 0 2 9 6 】

(付記 5 8) 所定の暗号処理がなされたアクセス要求を復号する第 1 の復号工程をさらに含み、前記第 1 の見積工程、事前判定工程または第 2 の見積工程は、前記第 1 の復号工程により復号されたアクセス要求について見積または判定をおこなうことを特徴とする付記 3 3 ～ 5 7 のいずれか一つに記載のフィルタリング方法。

【 0 2 9 7 】

(付記 5 9) 前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに

受け渡す場合に、前記第 1 の復号工程により復号されたアクセス要求ではなく、所定の暗号処理がなされたアクセス要求を前記サーバに受け渡すことを特徴とする付記 5 8 に記載のフィルタリング方法。

【 0 2 9 8 】

（付記 6 0）所定の暗号処理がなされたレスポンスを復号する第 2 の復号工程をさらに含み、前記レスポンス見積工程は、前記第 2 の復号工程により復号されたレスポンスについて見積をおこなうことを特徴とする付記 5 8 または 5 9 に記載のフィルタリング方法。

【 0 2 9 9 】

（付記 6 1）前記レスポンスのうちの正当なレスポンスのみを前記クライアントに送信する場合に、前記第 2 の復号工程により復号されたレスポンスではなく、所定の暗号処理がなされたレスポンスを前記クライアントに送信することを特徴とする付記 6 0 に記載のフィルタリング方法。

【 0 3 0 0 】

（付記 6 2）前記サーバに対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納した偽レスポンスデータベースを参照して、不正アクセスとして前記サーバに受け渡されなかったアクセス要求のパターンに対応した偽のレスポンスを作成する偽レスポンス作成工程と、前記偽レスポンス作成工程により作成された偽のレスポンスを前記クライアントに送信する偽レスポンス送信工程と、をさらに含んだことを特徴とする付記 3 3 ～ 6 1 のいずれか一つに記載のフィルタリング方法。

【 0 3 0 1 】

（付記 6 3）不正なアクセスとして前記サーバに受け渡されなかったアクセス要求を受け入れて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを前記サーバのおとりとして作成するおとり工程と、前記おとり工程により作成された偽のレスポンスを前記クライアントに送信する偽レスポンス送信工程と、をさらに含んだことを特徴とする付記 3 3 ～ 6 1 のいずれか一つに記載のフィルタリング方法。

【 0 3 0 2 】

(付記 6 4) 前記サーバに対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納した偽レスポンスデータベースを参照し、不正アクセスとして前記サーバに受け渡されなかったアクセス要求のうち、前記偽レスポンスデータベースに格納された不正アクセスのパターンに対応するアクセス要求について該パターンに対応した偽のレスポンスを作成する偽レスポンス作成工程と、不正アクセスとして前記サーバに受け渡されなかったアクセス要求のうち、前記偽レスポンスデータベースに格納された不正アクセスのパターンに対応しないアクセス要求を受け入れて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを前記サーバのおとりとして作成するおとり工程と、前記偽レスポンス作成工程または前記おとり工程により作成された偽のレスポンスを前記クライアントに送信する偽レスポンス送信工程と、をさらに含んだことを特徴とする付記 3 3 ～ 6 1 のいずれか一つに記載のフィルタリング方法。

【 0 3 0 3 】

(付記 6 5) 前記付記 3 3 ～ 6 4 のいずれか一つに記載された方法をコンピュータに実行させるプログラム。

【 0 3 0 4 】

【発明の効果】

以上説明したように、請求項 1、8 または 9 の発明によれば、サーバに対する不正アクセスのパターンを格納した不正パターンデータベースの不正アクセスのパターンおよび所定の見積ルールに基づいてアクセス要求の正当性を見積もり、この見積結果および所定の判定ルールに基づいてアクセス要求をサーバに受け渡すか否かを判定することとしたので、アクセス要求の送信元情報ではなくアクセス要求の具体的な要求内容に基づいて不正アクセスであるか否かを判定することができる。これにより、正当なアクセス要求のみをサーバに受け渡すことができ、もって不正クライアントと認定されていないクライアントからの不正アクセスに対してもサーバを防御することができる。

【 0 3 0 . 5 】

また、請求項 2 の発明によれば、アクセス要求が不正パターンデータベースに

格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、アクセス要求が不正パターンデータベースに格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、不正アクセスである旨が見積もられたアクセス要求をサーバに受け渡さないものと判定するとともに、正当アクセスである旨が見積もられたアクセス要求をサーバに受け渡すものと判定することとしたので、アクセス要求が不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを迅速かつ確実に判定することができ、もって不正クライアントと認定されていないクライアントからの不正アクセスに対しても迅速かつ確実にサーバを防御することができる。

【 0 3 0 6 】

また、請求項 3 の発明によれば、アクセス要求が不正パターンデータベースに格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、この算出された見積値と所定の閾値とを比較してアクセス要求をサーバに受け渡すか否かを判定することとしたので、見積値および閾値の比較によってある程度の幅を持たせて不正アクセスであるか否かを判定することができ、もって不正クライアントと認定されていないクライアントからの不正アクセスに対してもある程度の幅を持ってサーバを防御することができる。

【 0 3 0 7 】

また、請求項 4 の発明によれば、正当性を見積もりの前に、サーバに対する正当アクセスのパターンを格納した正当パターンデータベースを参照し、アクセス要求が正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定し、正当アクセスのパターンに該当しないもの判定されたアクセス要求のみについて正当性を見積もることとしたので、正当アクセスのパターンと一致するアクセス要求については正当性を見積もることなくサーバに受け渡す一方、正当アクセスのパターンと一致しないアクセス要求のみについて正当性を見積もることができ、もって不正アクセスであるか否かを全体としてより迅速に判定することができる。

【 0 3 0 8 】

また、請求項 5 の発明によれば、所定の外部送信ルールに基づいて、サーバに受け渡さないものと判定されたアクセス要求を所定の外部装置に送信することとしたので、不正アクセスに関する情報をサーバの管理者、フィルタリング装置の管理者、ネットワーク全般を監視する公的な機関の管理者などに迅速に送信することができ、もってかかる管理者に対しサーバの保全対策を迅速に促すことができる。

【 0 3 0 9 】

また、請求項 6 の発明によれば、所定の格納ルールに基づいて、サーバに受け渡さないものと判定されたアクセス要求を所定の格納媒体に格納することとしたので、格納媒体に格納された不正アクセスに関する情報を分析することなどができ、もってサーバの更なる保全対策を講じることができる。

【 0 3 1 0 】

また、請求項 7 の発明によれば、所定の更新ルールに基づいて、不正パターンデータベース、正当パターンデータベース、見積ルール、判定ルール、外部送信ルール、格納ルールまたは更新ルールを更新することとしたので、新たに発見された不正アクセスのパターンを不正パターンデータベースに登録することなどができ、もって日々進化する不正アクセスに対して機動的に対応することができる。

【図面の簡単な説明】

【図 1】

本実施の形態 1 に係るサーバクライアントシステムの構成を示すブロック図である。

【図 2】

不正リクエスト DB に格納される情報の構成例を示す図である。

【図 3】

本実施の形態 1 によるフィルタリングの処理手順を説明するフローチャートである。

【図 4】

本実施の形態 2 によるフィルタリングの処理手順を説明するフローチャートで

ある。

【図 5】

本実施の形態 3 に係るサーバクライアントシステムの構成を示すブロック図である。

【図 6】

本実施の形態 3 によるフィルタリングの処理手順を説明するフローチャートである。

【図 7】

本実施の形態 4 に係るサーバクライアントシステムの構成を示すブロック図である。

【図 8】

本実施の形態 4 によるフィルタリングの処理手順を説明するフローチャートである。

【図 9】

本実施の形態 4 の変形例に係るサーバクライアントシステムの構成を示すブロック図である。

【図 1 0】

本実施の形態 5 に係るサーバクライアントシステムの構成を示すブロック図である。

【図 1 1】

本実施の形態 6 に係るサーバクライアントシステムの構成を示すブロック図である。

【図 1 2】

本実施の形態 6 によるフィルタリングの処理手順を説明するフローチャートである。

【図 1 3】

本実施の形態 7 に係るサーバクライアントシステムの構成を示すブロック図である。

【図 1 4】

本実施の形態 8 に係るサーバクライアントシステムの構成を示すブロック図である。

【図 1 5】

本実施の形態 8 によるフィルタリングの処理手順を説明するフローチャートである。

【図 1 6】

本実施の形態 9 に係るサーバクライアントシステムの構成を示すブロック図である。

【図 1 7】

本実施の形態 9 によるフィルタリングの処理手順を説明するフローチャートである。

【図 1 8】

本実施の形態 1 0 に係るサーバクライアントシステムの構成を示すブロック図である。

【図 1 9】

本実施の形態 1 0 に係るサーバクライアントシステムの構成を示すブロック図である。

【符号の説明】

- 1 ネットワーク
- 1 0 クライアント装置
- 1 1 W e b ブラウザ
- 2 0、6 0 サーバ装置
- 3 0、7 0 リクエストフィルタ
- 3 1 受信部
- 3 2 見積部
- 3 2 a 見積ルール
- 3 3 不正リクエスト D B
- 3 4 判定部
- 3 4 a 判定ルール

- 3 5 送信部
- 3 6 ログ管理部
 - 3 6 a 管理ルール
- 3 7 外部通報部
 - 3 7 a 通報ルール
- 3 8 外部情報取得部
 - 3 8 a 取得ルール
- 3 9 更新部
 - 3 9 a 更新ルール
- 4 0 W e b サーバ
- 5 0 外部装置
- 7 1 事前判定部
 - 7 1 a 事前判定ルール
- 7 2 正当リクエストDB
- 8 0、9 0 サーバ装置
- 8 1、9 1 リクエストフィルタ
- 8 2 第 1 見積部
 - 8 2 a 見積ルール
- 8 3 不正リクエストDB
- 8 4 第 1 判定部
 - 8 4 a 判定ルール
- 8 5 第 1 見積部
 - 8 5 a 見積ルール
- 8 6 統計的不正リクエストDB
- 8 7 第 2 判定部
 - 8 7 a 判定ルール
- 8 8 送信部
- 1 0 0 サーバ装置
- 1 0 1 リクエストフィルタ

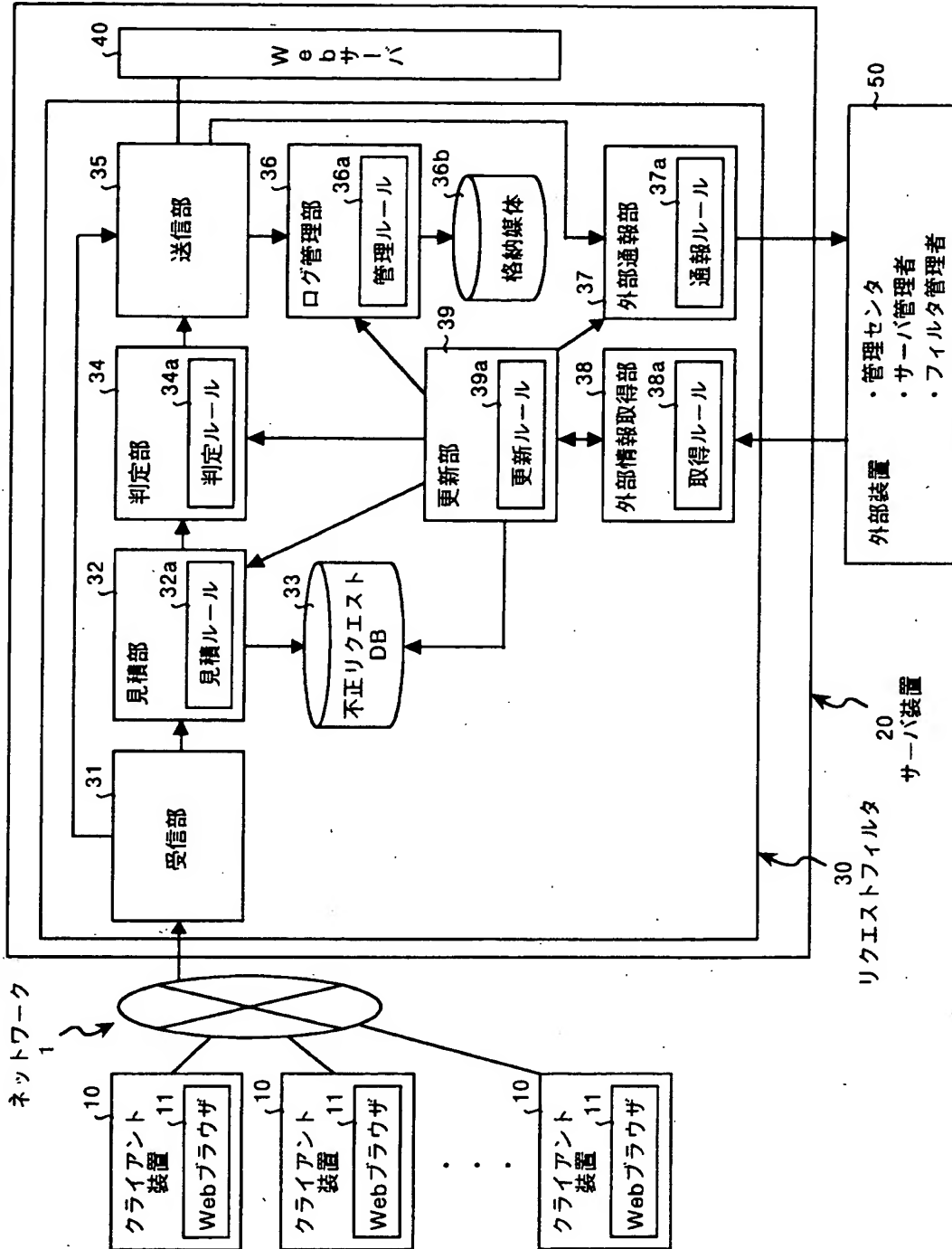
- 1 0 2 アクセス管理部
- 1 0 3 動的更新部
- 1 0 3 a 更新ルール
- 1 1 0、1 2 0 サーバ装置
- 1 1 1、1 2 1 リクエストフィルタ
- 1 1 2 レスポンス受信部
- 1 1 3 レスポンス見積部
- 1 1 3 a 見積ルール
- 1 1 4 不正レスポンスDB
- 1 1 5 レスポンス判定部
- 1 1 5 a 判定ルール
- 1 1 6 レスポンス送信部
- 1 2 2、1 2 3 復号部
- 1 3 0、1 4 0、1 5 0 サーバ装置
- 1 3 1、1 4 1、1 5 1 リクエストフィルタ
- 1 3 2、1 5 2 偽レスポンス作成部
- 1 3 2 a、1 5 2 a 作成ルール
- 1 3 3 偽レスポンスDB
- 1 3 4 レスポンス送信部
- 1 4 2 偽Webサーバ

【書類名】

図面

【図 1】

本実施の形態 1 に係るサーバクライアントシステムの構成を示すブロック図



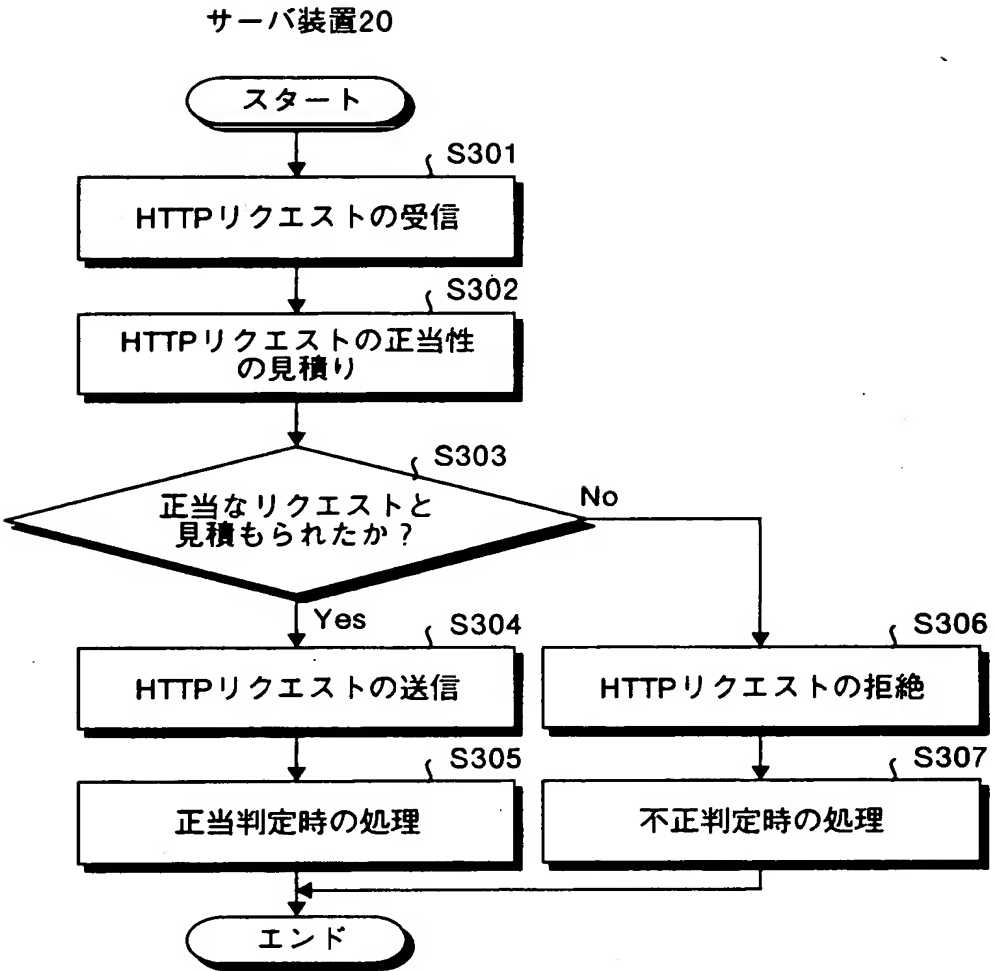
【図2】

不正リクエストDBに格納される情報の構成例を示す図

形式言語パターン	意味
URL=<//	URLの先頭が“//”と一致するリクエストを却下。
CGI=phf ARG=<Qname=root%OA	CGI名が“phf”であり、且つそのある引数の先頭が“Qname=root%OA”と一致するリクエストを却下。
URL<>..%..%..	URLに“..%..%..”が含まれるリクエストを却下。
CGI>=.htr	CGI名の末尾が、“htr”と一致するリクエストを却下。 すなわち、CGIが拡張子“.htr”を有するリクエストを却下。

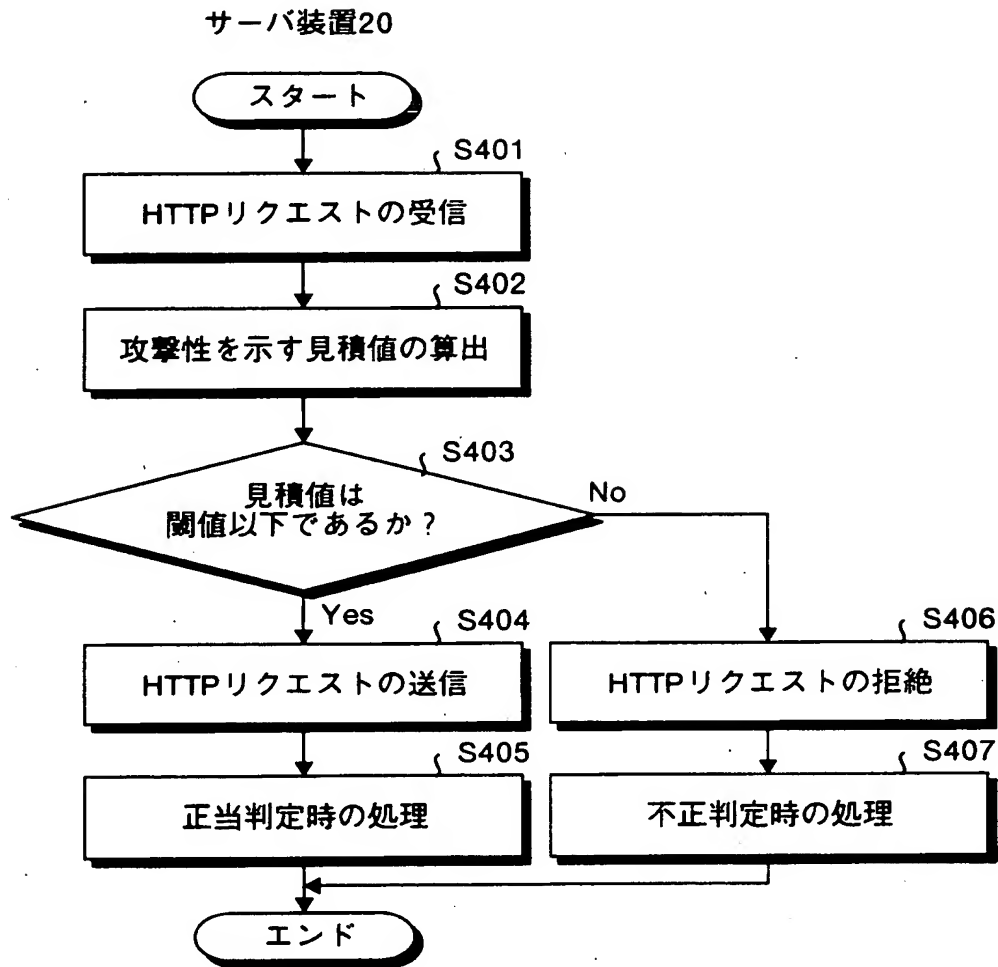
【図 3】

本実施の形態 1 によるフィルタリングの処理手順を示すフローチャート



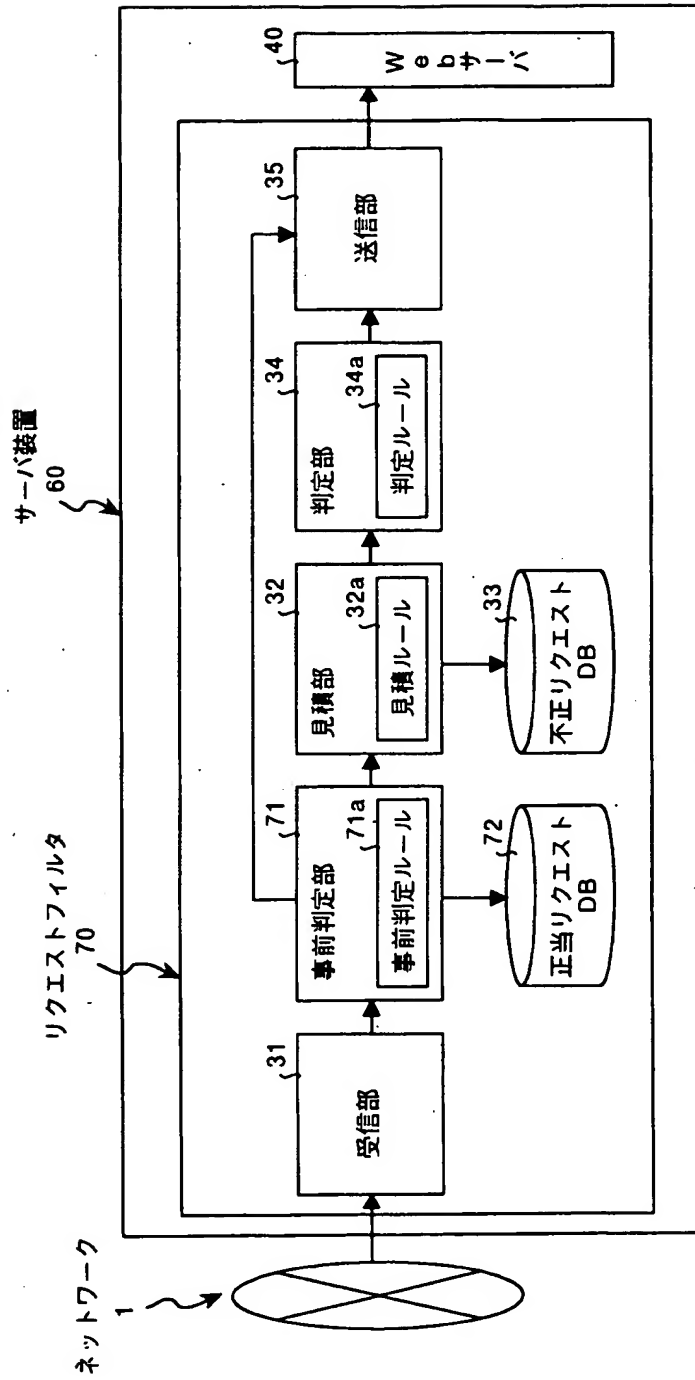
【図 4】

本実施の形態 2 によるフィルタリングの処理手順を示すフローチャート

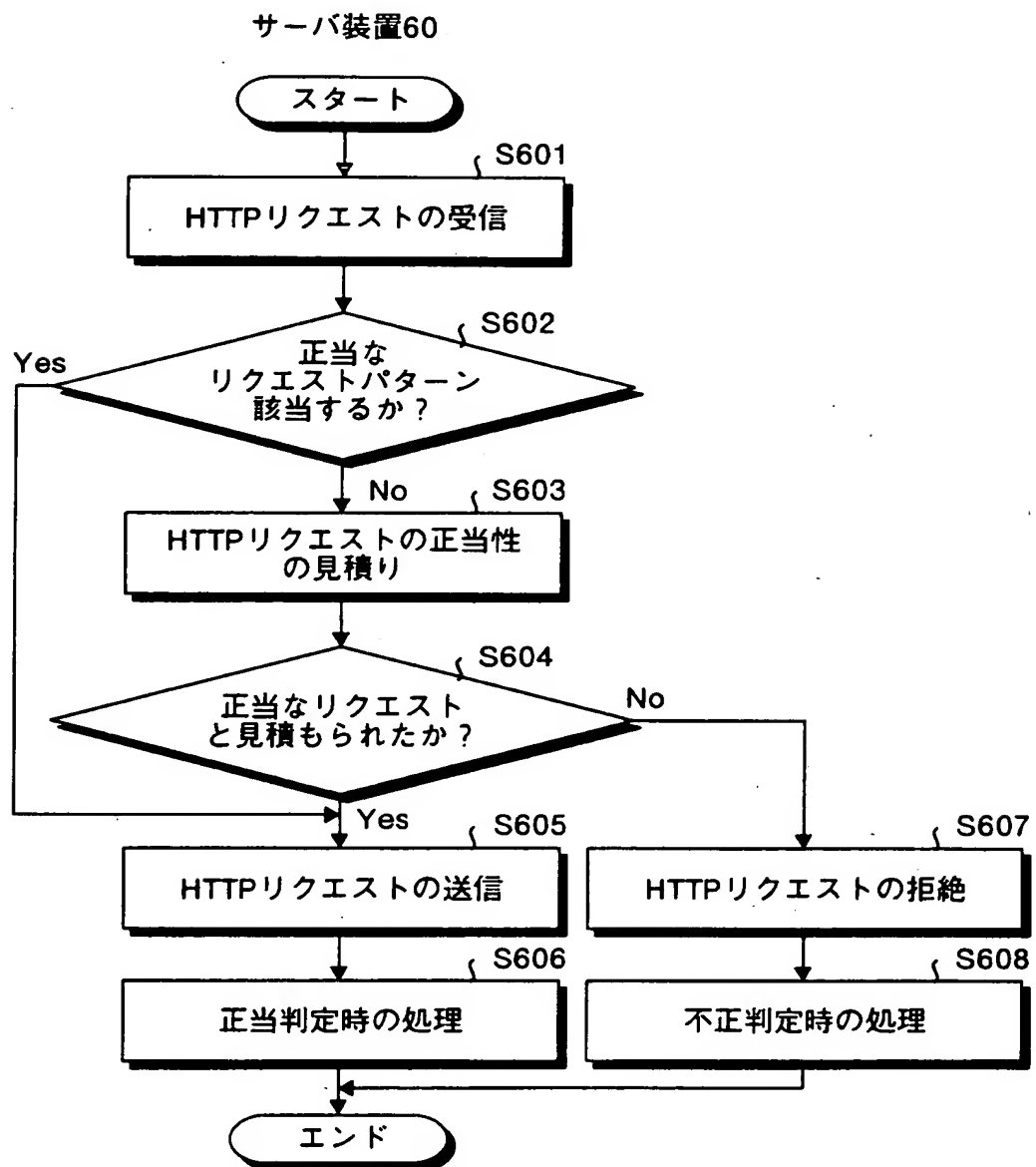


【図 5】

本実施の形態 3 に係るサーバクライアントシステムの構成を示すブロック図

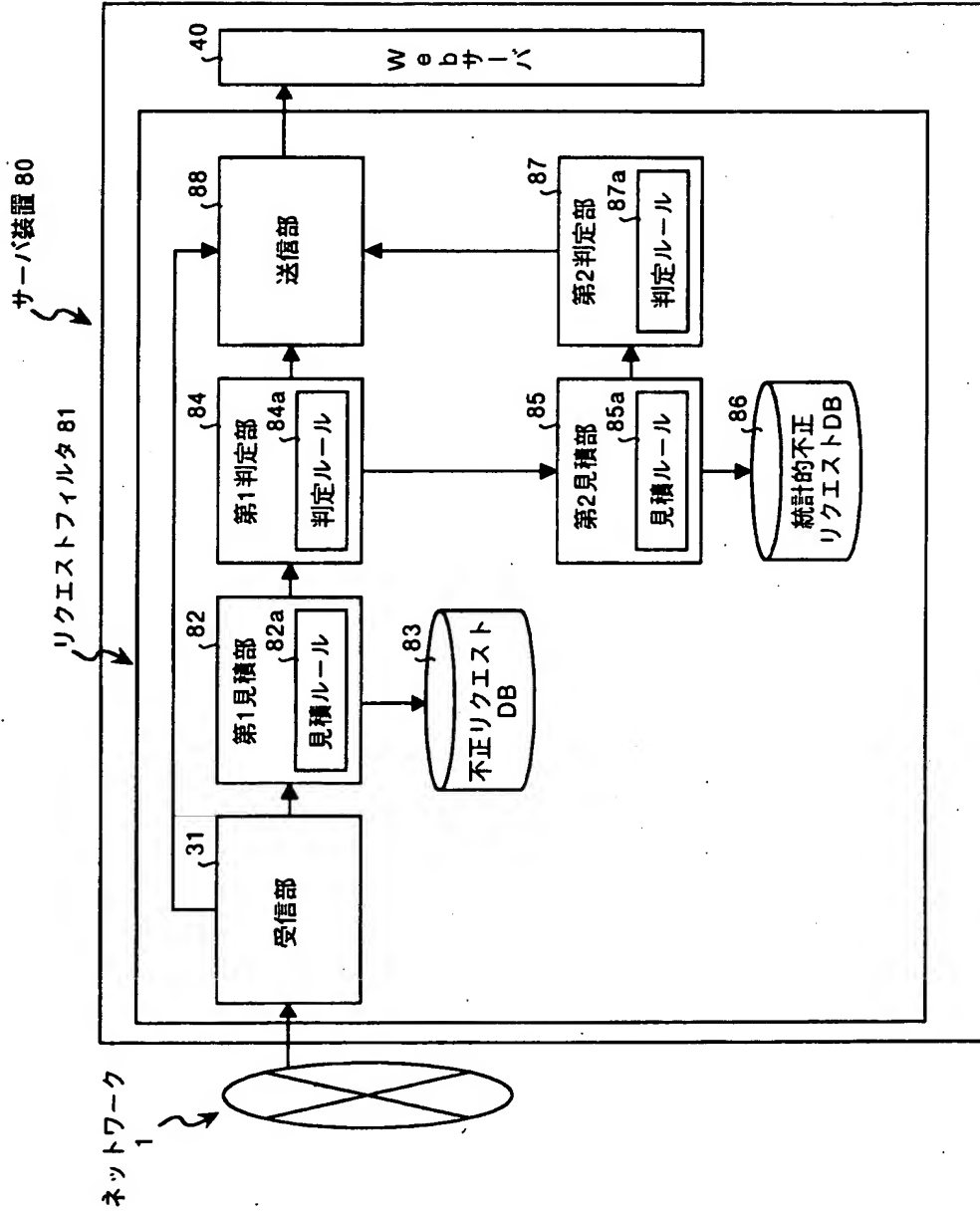


本実施の形態 3 によるフィルタリングの処理手順を示すフローチャート



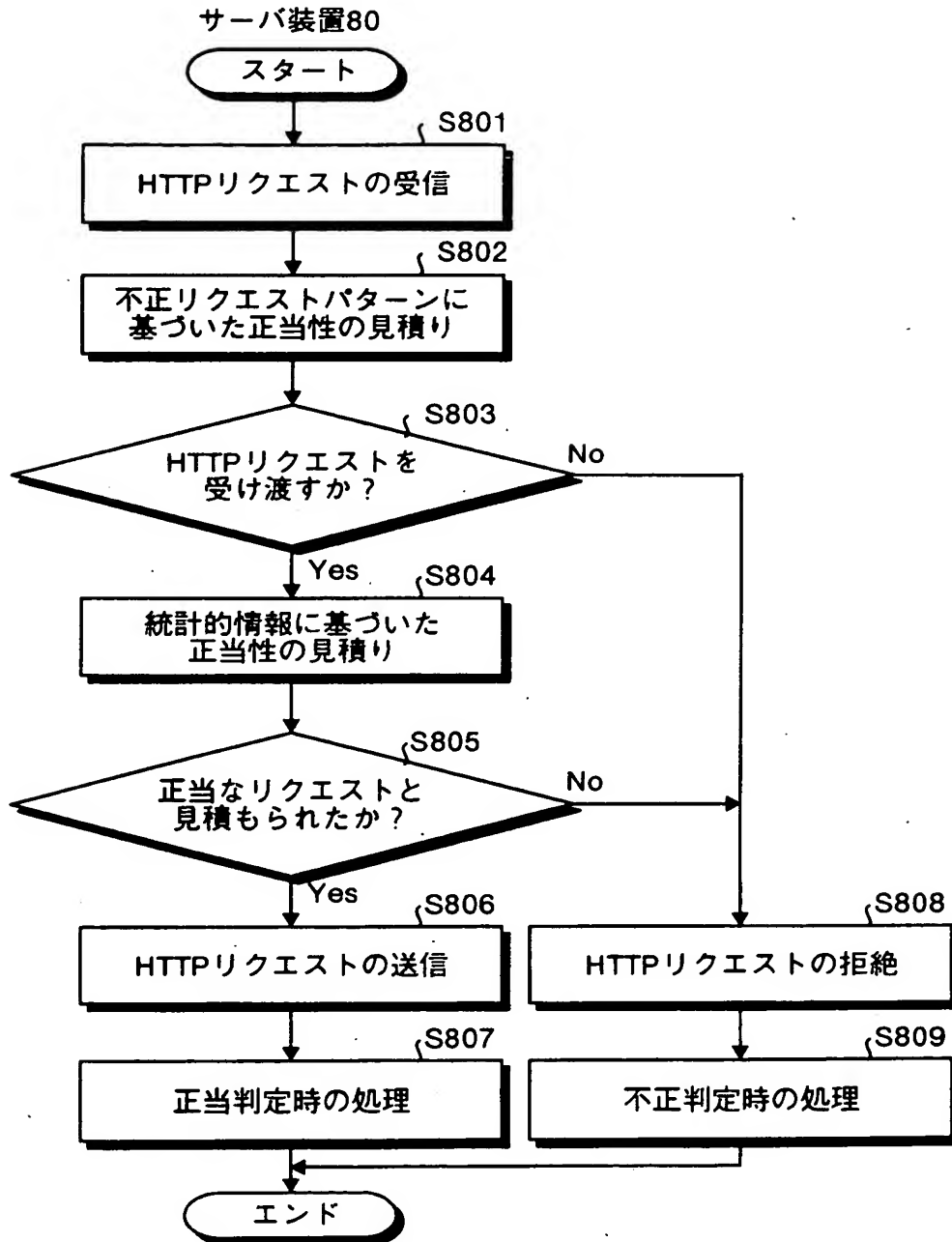
【図 7】

本実施の形態4に係るサーバクライアントシステムの構成を示すブロック図



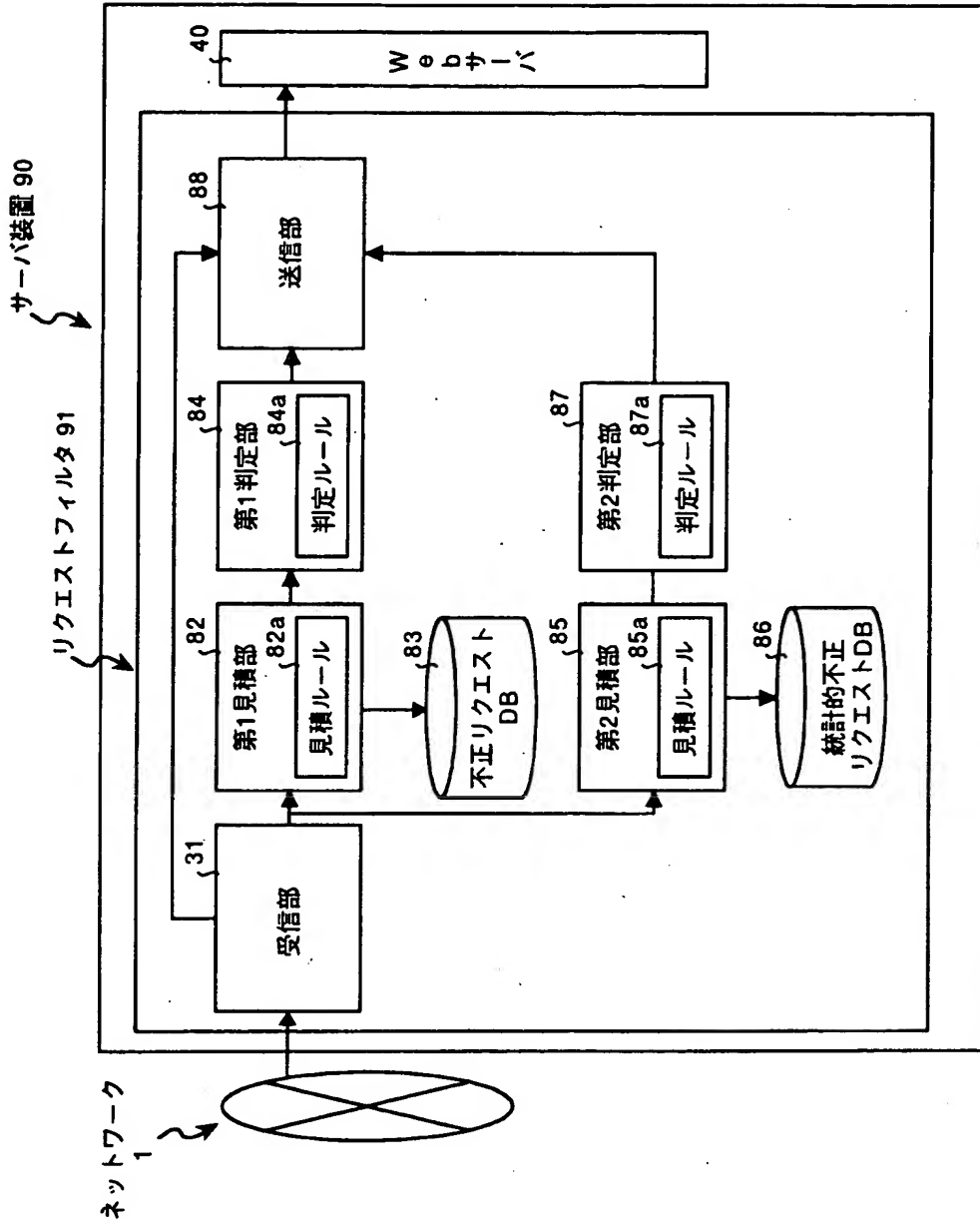
【図 8】

本実施の形態4によるフィルタリングの処理手順を示すフローチャート



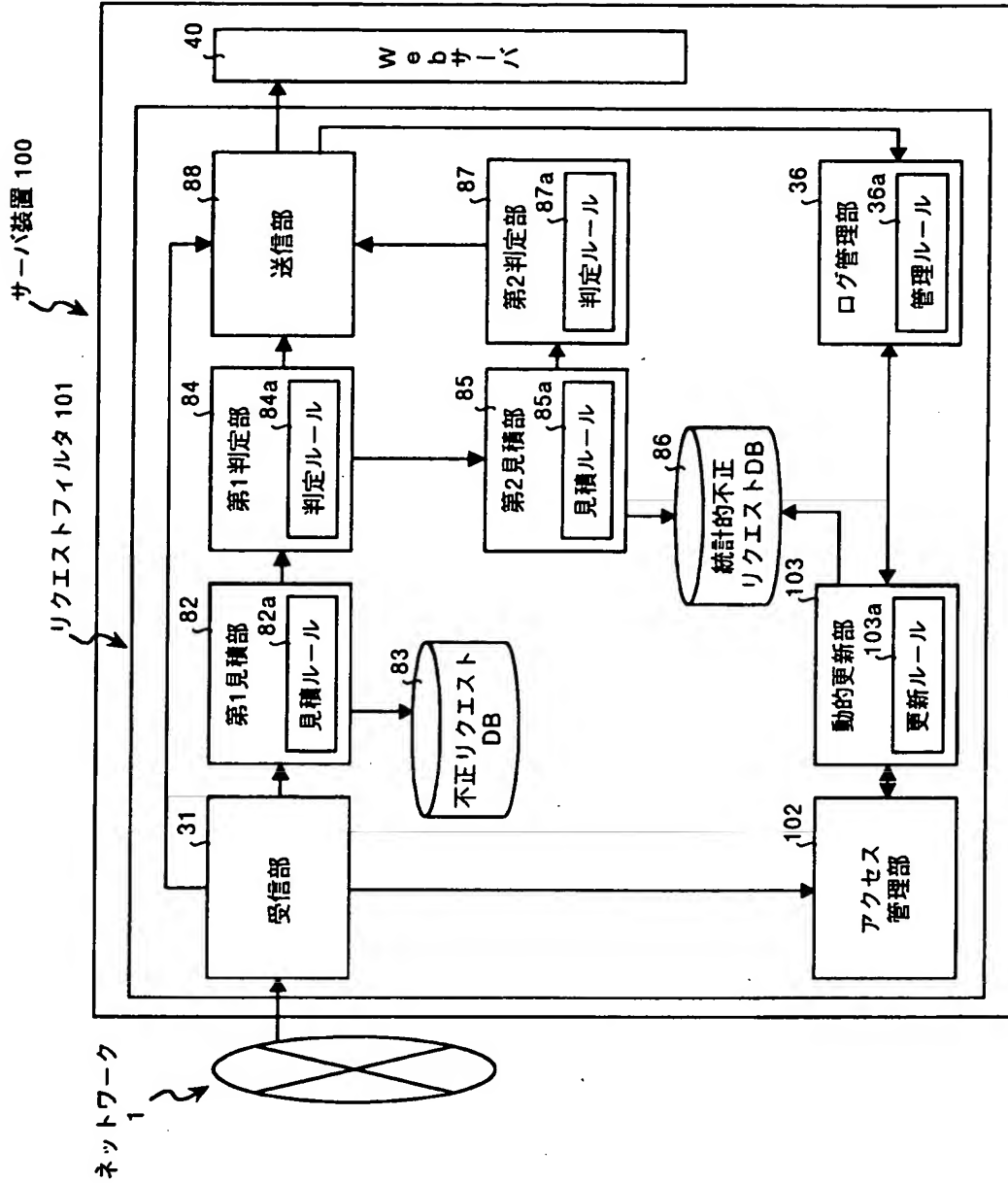
【図 9】

本実施の形態4の変形例に係るサーバクライアントシステムの構成を示すブロック図



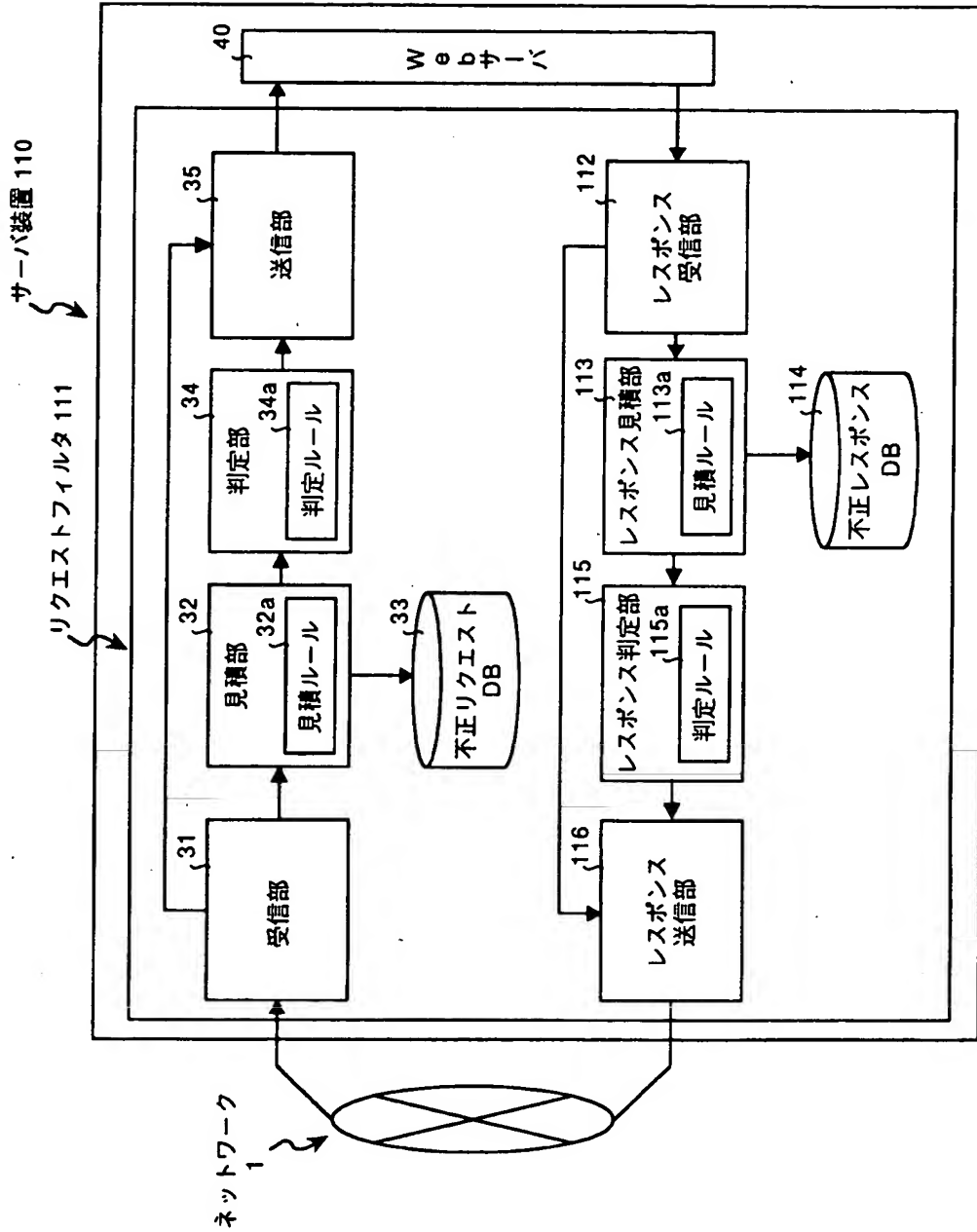
【図10】

本実施の形態5に係るサーバクライアントシステムの構成を示すブロック図



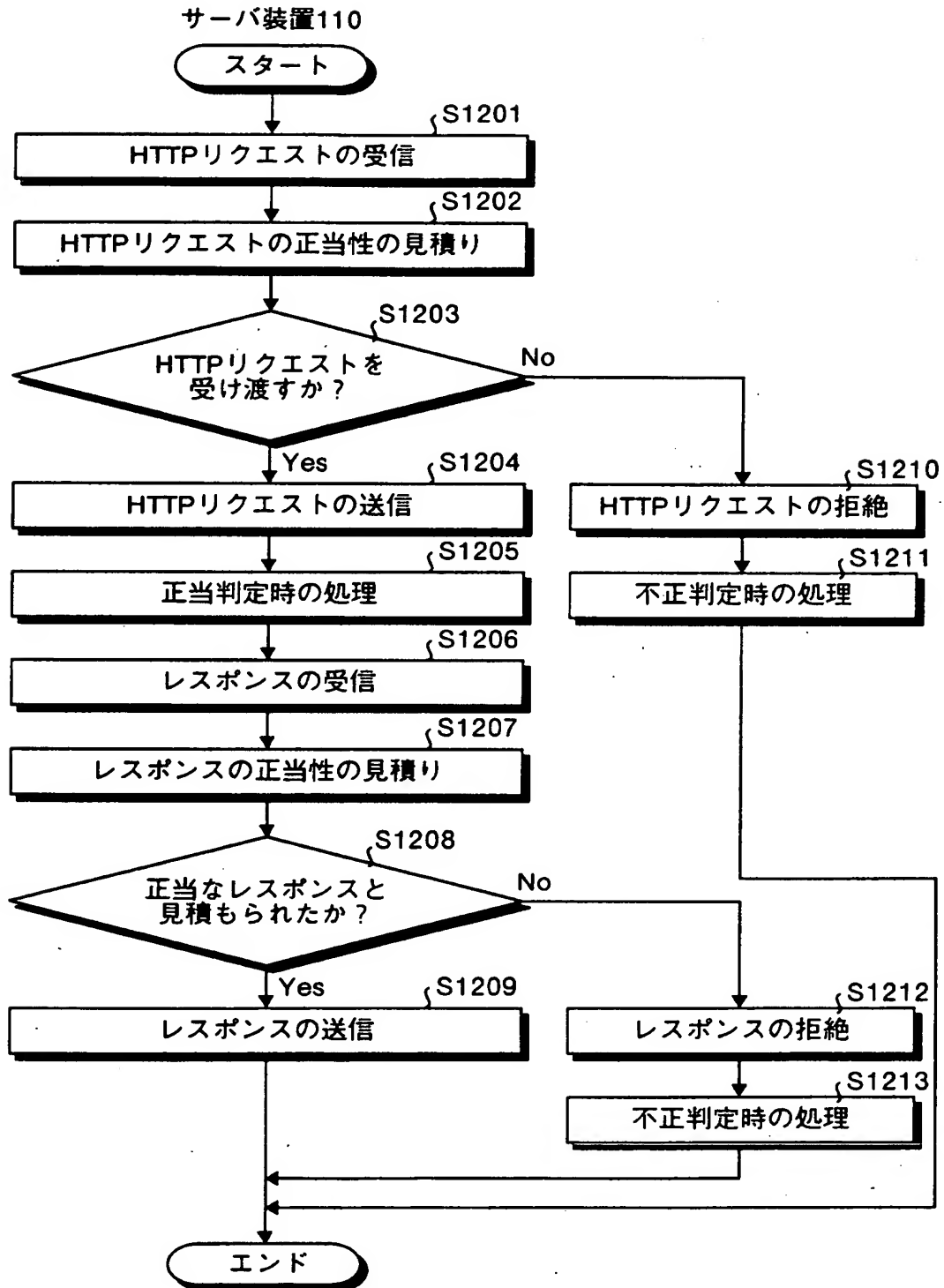
【図 1 1】

本実施の形態6に係るサーバクライアントシステムの構成を示すブロック図



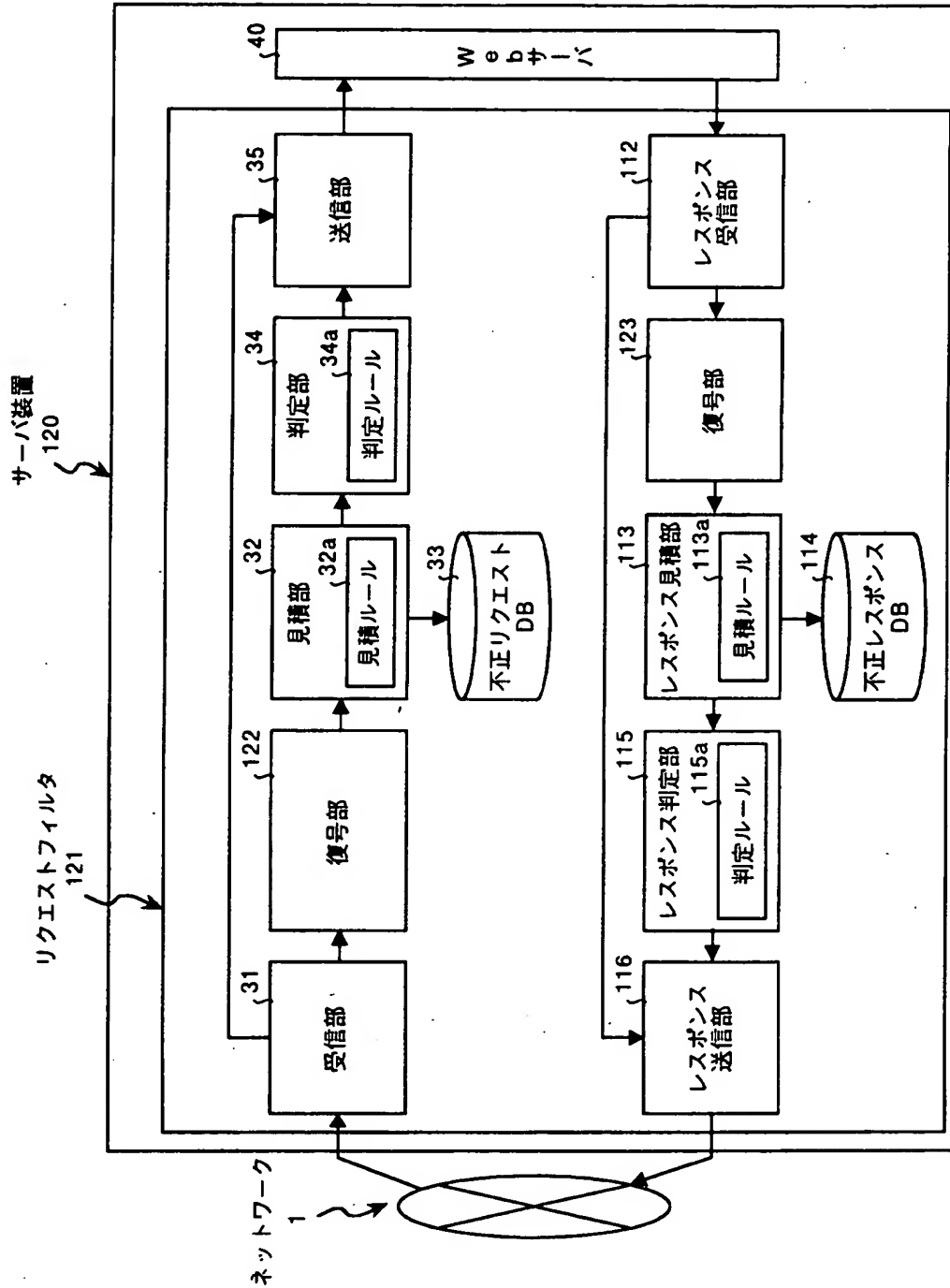
【図 1 2】

本実施の形態6によるフィルタリングの処理手順を示すフローチャート



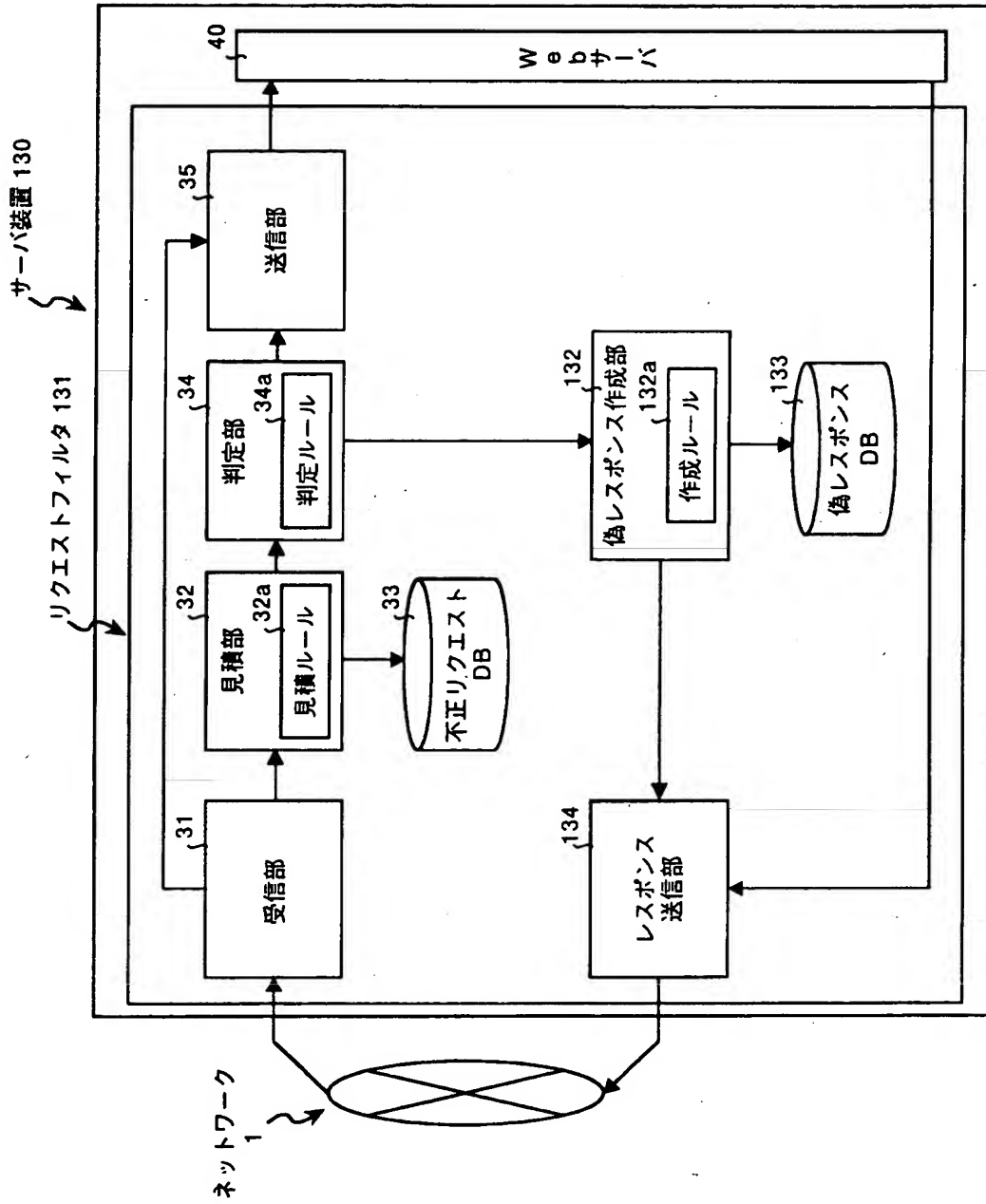
【図 13】

本実施の形態7に係るサーバライアントシステムの構成を示すブロック図



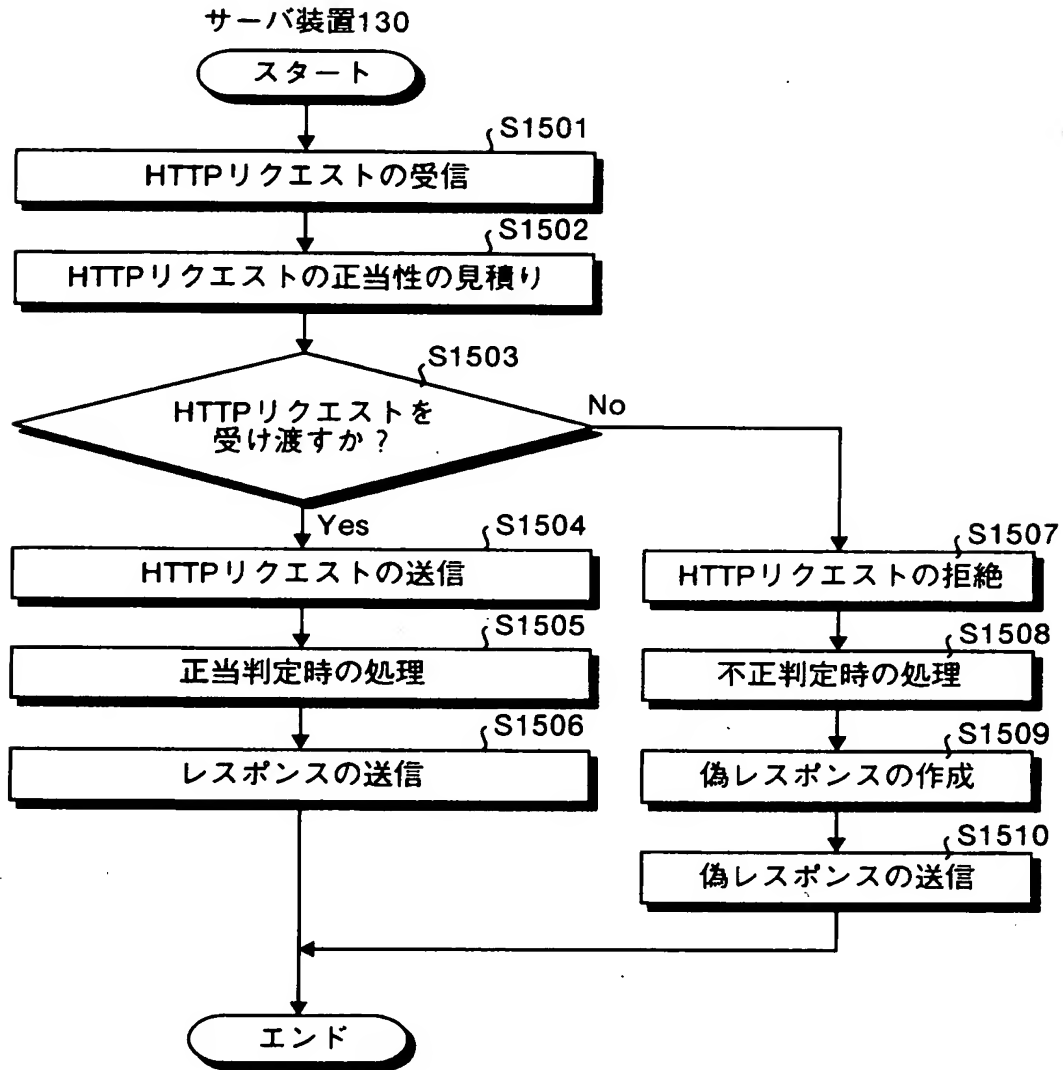
【図 14】

本実施の形態8に係るサーバクライアントシステムの構成を示すブロック図



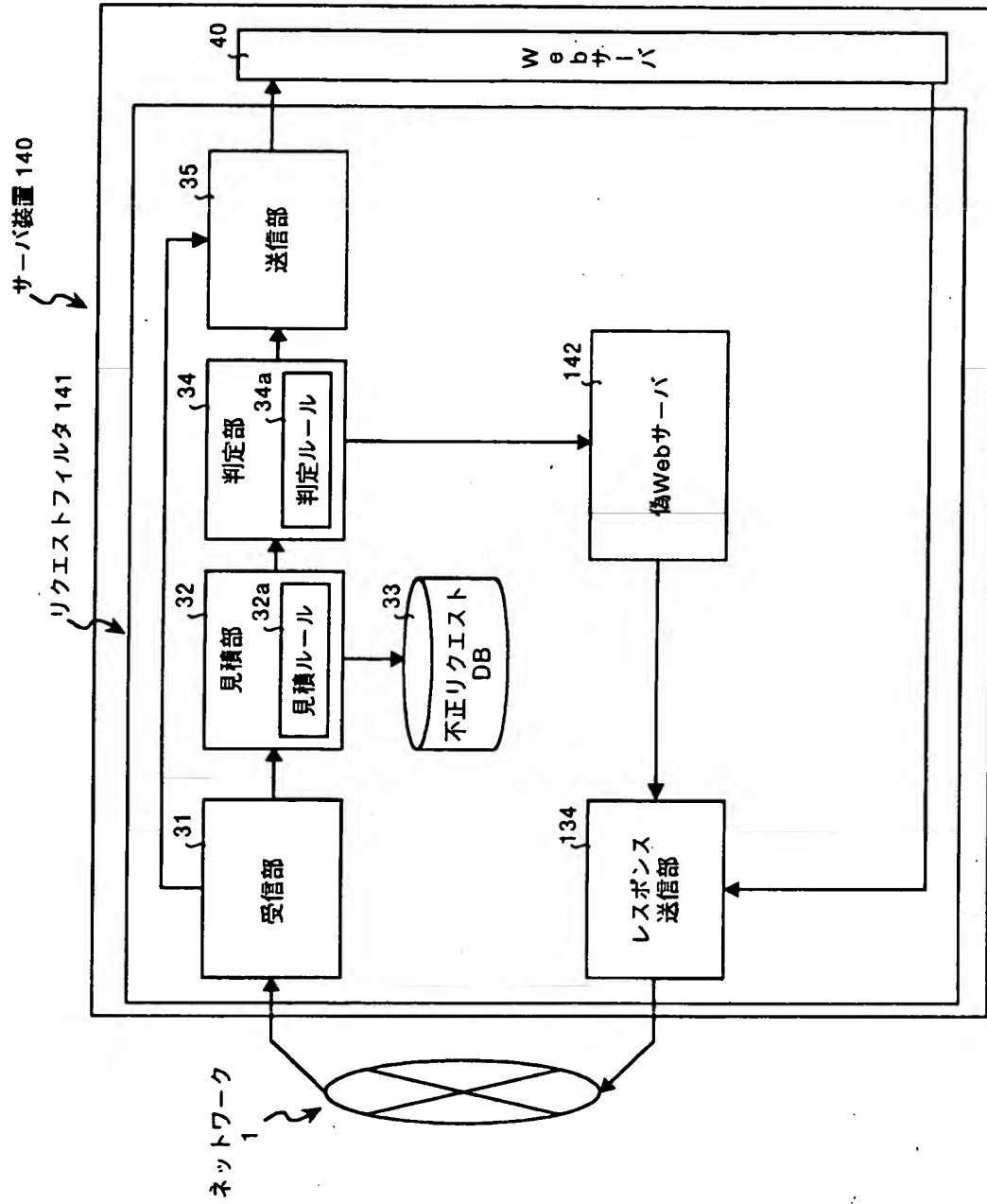
【図 1 5】

本実施の形態8によるフィルタリングの処理手順を示すフローチャート



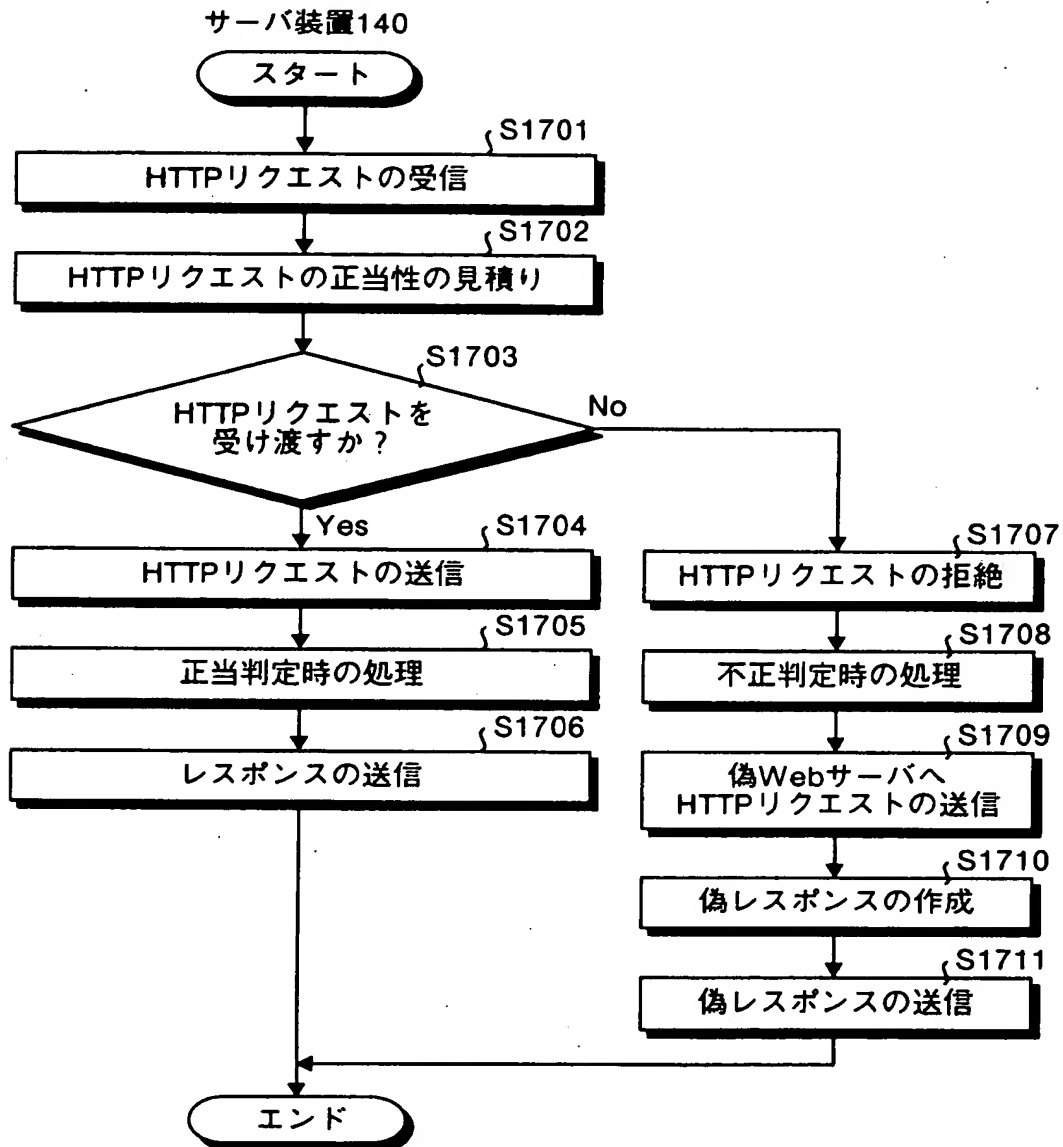
【図16】

本実施の形態9に係るサーバクライアントシステムの構成を示すブロック図



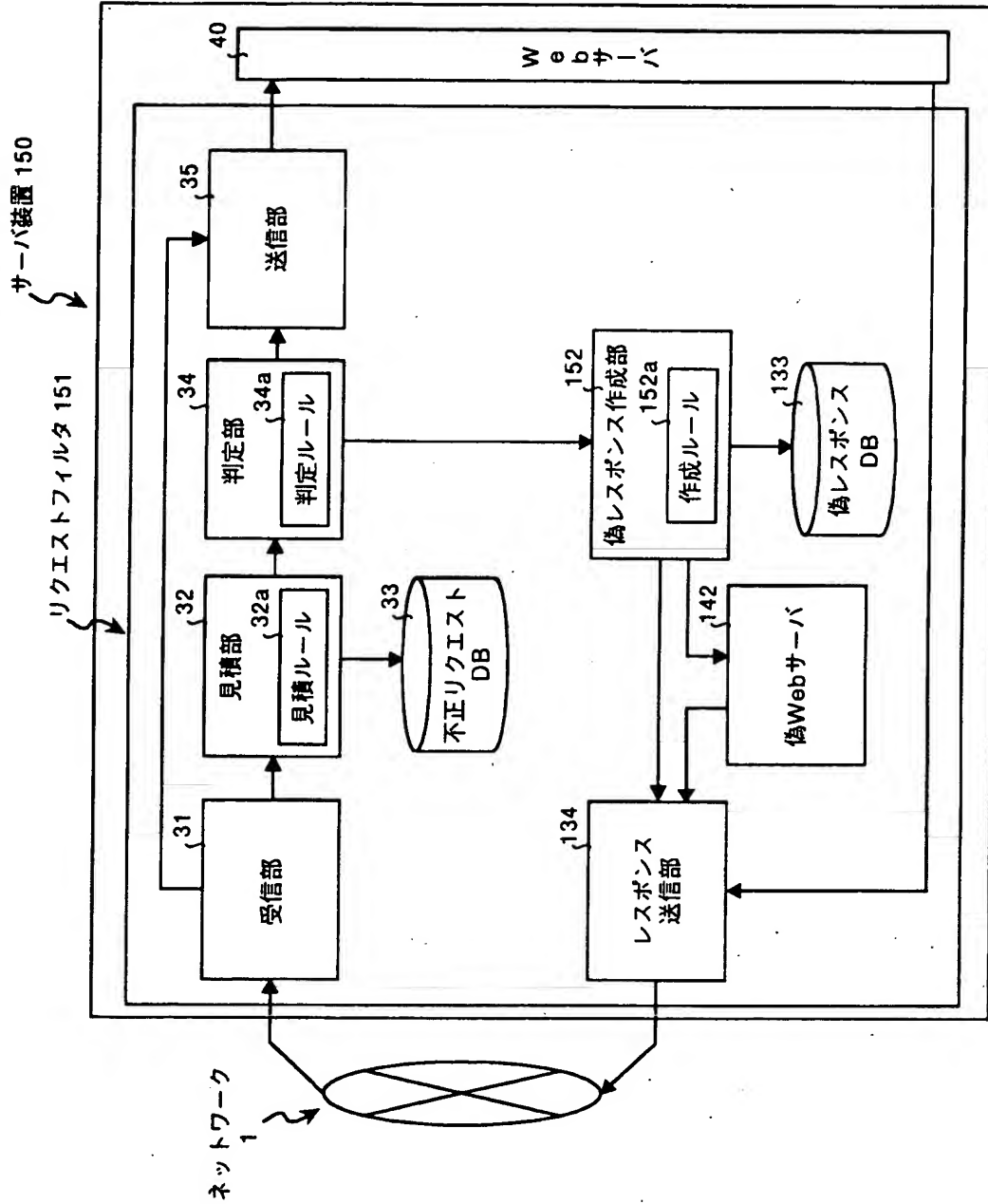
【図 1 7】

本実施の形態9によるフィルタリングの処理手順を示すフローチャート



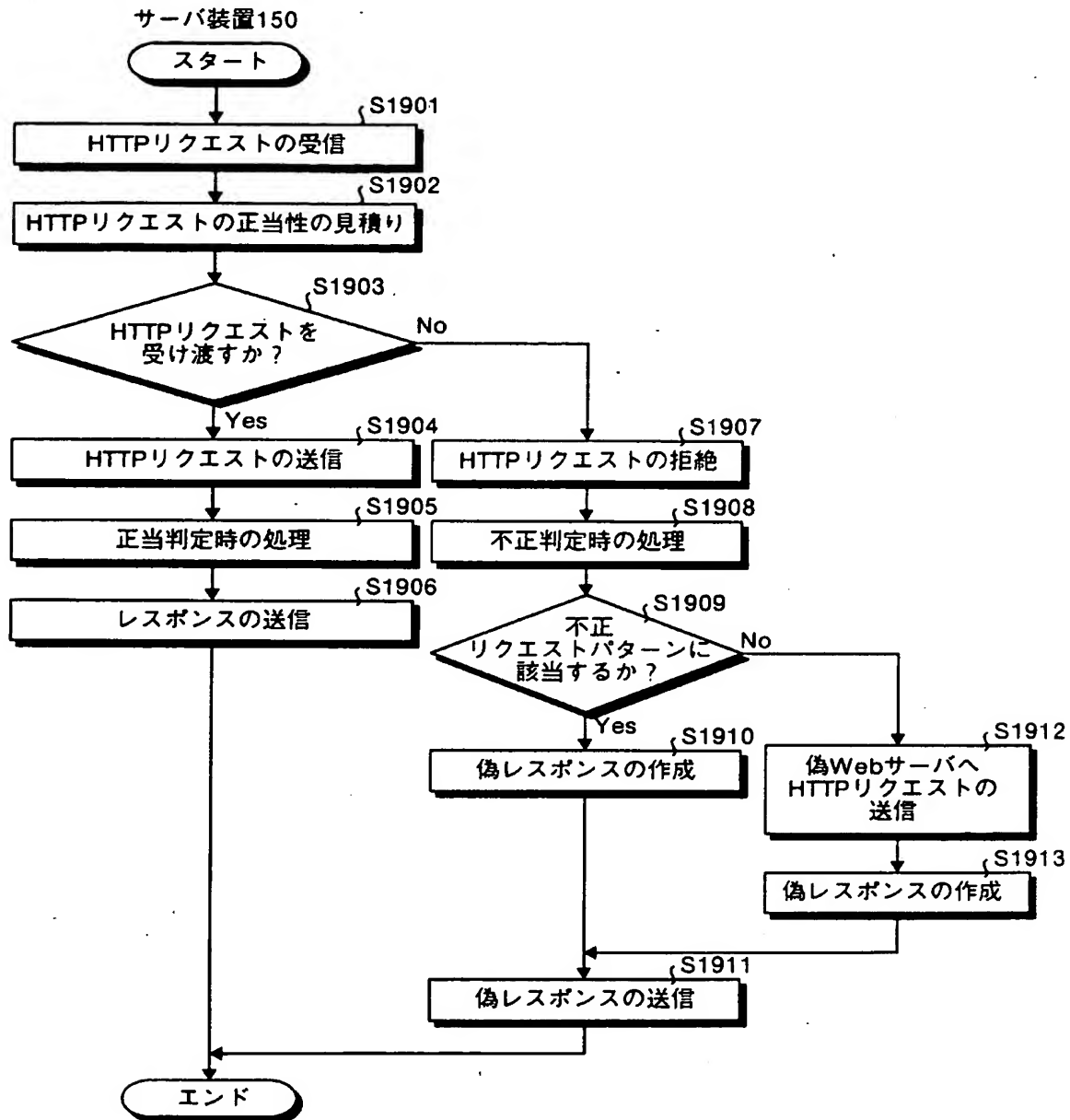
【図 1 8】

本実施の形態10に係るサーバクライアントシステムの構成を示すブロック図



【図 1 9】

本実施の形態10によるフィルタリングの処理手順を示すフローチャート



【書類名】 要約書

【要約】

【課題】 不正クライアントと認定されていないクライアントからの不正アクセスに対してもサーバを防御すること。

【解決手段】 Webサーバ40に対する不正アクセスのパターンを格納した不正リクエストDB（データベース）33と、不正リクエストDB33に格納された不正アクセスのパターンおよび所定の見積ルール32aに基づいてクライアント装置10からのアクセス要求の正当性を見積もる見積部32と、見積部32による見積結果および所定の判定ルール34aに基づいてアクセス要求をWebサーバ40に受け渡すか否かを判定する判定部34とを備える。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号
氏 名 富士通株式会社